National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
16 - 31 Oct 2022 Vol. 09 No. 20

Table of Content

Vendor	Product	Page Number
Application		
10web	form_maker	1
74cms	74cmsse	1
abpressoptimizer	ab_press_optimizer	2
adenion	blog2social	3
adminpad_project	adminpad	3
Adobe	commerce	4
	illustrator	6
Advantech	r-seenet	8
aethon	tug_home_base_server	9
Algosec	fireflow	10
alivecor	kardia	11
anji-plus	report	12
Apache	batik	12
	dolphinscheduler	13
	dubbo	13
	flume	14
	geode	15
	heron	15
	iotdb	16
	isis	16
	linkis	20
ARM	bifrost_gpu_kernel_driver	21
	midguard_gpu_kernel_driver	21
	valhall_gpu_kernel_driver	22
Asus	asusliveupdate	23
	asussoftwaremanger	23
	asusswitch	24

Vendor	Product	Page Number
Asus	system_control_interface	24
Autodesk	autocad	25
	autocad_advance_steel	52
	autocad_architecture	78
	autocad_civil_3d	105
	autocad_electrical	132
	autocad_lt	158
	autocad_map_3d	185
	autocad_mechanical	212
	autocad_mep	238
	autocad_plant_3d	265
	design_review	292
automox	automox	297
Avira	avira_security	297
axiosys	bento4	298
Baramundi	management_suite	304
barangay_management_system_project	barangay_management_system	304
Bestwebsoft	post_to_csv	305
best_student_result_management_system_project	best_student_result_management_system	305
billing_system_project	billing_system	305
bookstackapp	bookstack	306
boxbilling	boxbilling	306
bricksbuilder	bricks	307
canteen_management_system_project	canteen_management_system	307
cashier_queuing_system_project	cashier_queuing_system	310
cert	vince	311
Chamilo	chamilo	311
changingtec	rava_certificate_validation_system	312
chop-chop	pop-up_chop_chop	313

Vendor	Product	Page Number
Cisco	identity_services_engine	314
	telepresence_collaboration_endpoint	319
cleantalk	spam_protection\,_antispam\,_firewall	322
cloudflare	octorpki	322
	warp	323
	warp_mobile_client	324
codedropz	drag_and_drop_multiple_file_upload_-_contact_form_7	324
codexpert	search_logger	325
Dart	dart_software_development_kit	325
dataease	dataease	326
datahub_project	datahub	327
Dell	emc_isilon_onefs	328
deltaww	diaenergie	328
designextreme	we\'re_open	331
Devexpress	asp.net_web_forms_controls	331
devhubapp	devhub	332
discourse	patreon	332
Djangoproject	django	333
dzzoffice	dzzoffice	334
Eclipse	openj9	334
edetw	u-office_force	335
ehoney_project	ehoney	337
elearning_system_project	elearning_system	339
emlog	emlog	339
employee_record_management_system_project	employee_record_management_system	340
Enalean	tuleap	340
Esri	arcgis_server	342
eve-ng	eve-ng	346
evm_project	evm	346
Exim	exim	347

Vendor	Product	Page Number
Exiv2	exiv2	348
expresstech	quiz_and_survey_master	350
extended_keccak_code_package_project	extended_keccak_code_package	352
eyoucms	eyoucms	352
F5	big-ip_access_policy_manager	353
	big-ip_advanced_firewall_manager	363
	big-ip_advanced_web_application_firewall	375
	big-ip_analytics	379
	big-ip_application_acceleration_manager	390
	big-ip_application_security_manager	400
	big-ip_application_visibility_and_reporting	413
	big-ip_carrier-grade_nat	415
	big-ip_ddos_hybrid_defender	416
	big-ip_domain_name_system	418
	big-ip_edge_gateway	430
	big-ip_fraud_protection_service	432
	big-ip_global_traffic_manager	442
	big-ip_link_controller	452
	big-ip_local_traffic_manager	463
	big-ip_policy_enforcement_manager	475
	big-ip_ssl_orchestrator	486
	big-ip_webaccelerator	488
	big-ip_websafe	490
	big-iq_centralized_management	492
	nginx	493
	nginx_ingress_controller	503
	nginx_plus	508
	njs	508
fatcatapps	analytics_cat	509
featherjs	feathers-sequelize	510
flutter	flutter	511
fluxcd	flux2	511

Vendor	Product	Page Number
fluxcd	helm-controller	512
	image-automation-controller	514
	image-reflector-controller	514
	kustomize-controller	515
	notification-controller	517
	source-controller	518
Forgerock	access_management	520
Fortinet	fortiproxy	523
	fortiswitchmanager	526
	fortitester	527
free5gc	free5gc	533
fujielectric	d300win	534
garage_management_system_project	garage_management_system	534
genivi	diagnostic_log_and_trace	535
Get-simple	getsimple_cms	536
Getkirby	Kirby	536
gin-vue-admin_project	gin-vue-admin	542
Git-scm	git	544
gitea	gitea	567
Github	enterprise_server	568
	runner	570
Gitlab	gitlab	576
gl-inet	goodcloud	607
GNU	libtasn1	608
go-admin	go-admin	608
Google	bazel	609
	drive	609
gpac	gpac	610
Gradle	enterprise	612
hashicorp	boundary	612
Haxx	curl	612
helpful_project	helpful	613

Vendor	Product	Page Number
hiwin	robot_system_software	614
hornerautomation	cscape	614
hospital_management_system_project	hospital_management_system	616
hunter2_project	hunter2	617
IIJ	iij_smartkey	617
ikus-soft	rdiffweb	618
Ipfire	ipfire	619
jadx_project	jadx	619
Jenkins	360_fireline	620
	compuware_source_code_download_for_endevor\,_pds\,_and_ispw	620
	compuware_strobe_measurement	621
	compuware_topax_for_total_test	621
	compuware_topaz_for_total_test	622
	compuware_topaz_utilities	622
	compuware_xpediter_code	623
	contrast_continuous_application_security	623
	custom_checkbox_parameter	624
	generic_webhook_trigger	624
	groovy	625
	groovy_libraries	626
	input_step	627
	jenkins	627
	job_import	632
	katalon	633
	mercurial	635
	neuvector_vulnerability_scanner	635
	nunit	635
	repo	636
	s3_explorer	636
	screenrecorder	636
	script_security	637

Vendor	Product	Page Number
Jenkins	stage_view	638
	supporting_apis	639
	tuleap_git_branch_source	639
	xframium_builder	639
jflyfox	jfinal_cms	640
jhead_project	jhead	640
Joomla	joomla\!	640
jsonlint_project	jsonlint	641
Juiker	juiker	641
Juniper	paragon_active_assurance_control_center	642
Jupyter	jupyter_core	643
kadencewp	kadence_woocommerce_email_designer	644
kartverket	github-workflows	644
keking	kkfileview	645
keystonejs	keystone	646
Laubrotel	lbstopattack	646
lavalite	lavalite	647
lemon8_project	lemon8	647
libexpat_project	libexpat	648
Libtiff	libtiff	648
Liferay	dxp	651
	liferay_portal	656
Litespeedtech	openlitespeed	659
Magento	magento	661
markdownify_project	markdownify	663
Mcafee	epolicy_orchestrator	664
megazone	reversewall-mds	666
mekshq	meks_easy_social_share	666
merchandise_online_store_project	merchandise_online_store	666
metabase	metabase	667
Microsoft	azure_command-line_interface	688
mindskip	xzs	688

Vendor	Product	Page Number
minimatch_project	minimatch	689
miniorange	discord_integration	689
Mitel	micollab	690
Mitre	caldera	691
Najeebmedia	frontend_file_manager_plugin	692
Nextcloud	nextcloud_enterprise_server	693
	nextcloud_server	696
nopcommerce	nopcommerce	698
ocomon_project	ocomon	699
octoprint	octoprint	699
octopus	octopus_server	700
online_medicine_ordering_system_project	online_medicine_ordering_system	702
online_pet_shop_we_app_project	online_pet_shop_we_app	703
online_tours_and_travels_management_system_project	online_tours_and_travels_management_system	704
online_tours_\&_travels_management_system_project	online_tours_\&_travels_management_system	704
Open-xchange	ox_app_suite	704
openbmc-project	openbmc	705
opencats	opencats	706
opencrx	opencrx	709
openfga	openfga	709
opensecurity	mobile_security_framework	710
Opensuse	factory	711
opensvc	multipath-tools	711
open_source_sacco_management_system_project	open_source_sacco_management_system	713
Oracle	access_manager	713
	applications_framework	715
	bi_publisher	715

Vendor	Product	Page Number
Oracle	business_intelligence	719
	communications_billing_and_revenue_management	720
	database	721
	database_-_sharding	722
	database_server	723
	e-business_suite	724
	enterprise_data_quality	725
	enterprise_manager_base_platform	732
	graalvm	734
	http_server	760
	java_virtual_machine	762
	jdk	763
	jd_edwards_enterpriseone_tools	788
	jre	791
	mysql	815
	peoplesoft_enterprise	836
	peoplesoft_enterprise_common_components	841
	peoplesoft_enterprise_peopletools	842
	siebel_core_-_db_deployment_and_configuration_accessible_data	844
	soa_suite	845
	transportation_management	846
	vm_virtualbox	852
	weblogic_server	860
	web_applications_desktop_integrator	863
oroinc	orocommerce	863
osgeo	shapelib	865
Otrs	otrs	865
Owasp	dependency-track	866
	dependency-track_frontend	867
oxilab	accordions	869

Vendor	Product	Page Number
Paessler	prtg_network_monitor	869
parseplatform	parse-server	870
passster_project	passster	871
password_storage_application_project	password_storage_application	871
pctechsoft	pcsecure	872
phoenixframework	phoenix	872
Phpmyfaq	phpmyfaq	872
phpok	phpok	873
pikepdf_project	pikepdf	873
Pimcore	pimcore	874
Pivotal	reactor_netty	874
Pulpproject	pulp_ansible	875
pwndoc_project	pwndoc	875
pytest	py	876
Qemu	qemu	876
ragic	ragic	876
Redhat	3scale_api_management	877
	ansible_automation_platform	877
	satellite	877
	update_infrastructure	878
	virtualization	878
redis	redis	878
relatedcode	messenger	880
retain	retain_live_chat	880
Rockwellautomation	factorytalk_alarms_and_events	881
	factorytalk_vantagepoint	881
Rubyonrails	rails	886
rukovoditel	rukovoditel	887
sanitization_management_system_project	sanitization_management_system	888

Vendor	Product	Page Number
school_activity_updates_with_sms_notification_project	school_activity_updates_with_sms_notification	890
Sem-cms	Semcms	890
shescape_project	shescape	893
shinken-monitoring	shinken_monitoring	894
Siemens	jt2go	894
	siveillance_video_mobile_server	895
	teamcenter_visualization	895
simple_cold_storage_management_system_project	simple_cold_storage_management_system	896
	simple_cold_storage_managment_system	900
simple_exam_reviewer_management_system_project	simple_exam_reviewer_management_system	900
simple_online_public_access_catalog_project	simple_online_public_access_catalog	902
Smackcoders	an_ultimate_wordpress_importer_cum_migration_as_csv_\&_xml	902
socket	socket.io-parser	903
soflyy	wp_all_export	903
Softing	edgeaggregator	904
	edgeconnector	904
	opc	905
	opc_ua_c\+\+_software_development_kit	905
	secure_integration_server	906
	uagates	906
softmotions	iowow	907
softr	softr	907
Solarwinds	orion_platform	908
	sql_sentry	913
Sony	content_transfer	914
sra-admin_project	sra-admin	914
ST	stm32_mw_usb_host	915

Vendor	Product	Page Number
superwhite	demon_image_annotation	915
synacor	zimbra_collaboration_suite	916
Synology	diskstation_manager	916
	presto_file_server	919
tableau	tableau_server	920
tasks	tasks	923
Tech-banker	contact_bank	925
Tenable	nessus	926
themepoints	testimonials	927
themeum	tutor_lms	927
train_scheduler_app_project	train_scheduler_app	928
trumpf	job_order_interface	928
	oseon	929
	trutops_boost	929
	trutops_fab	929
	trutops_monitor	930
twistedmatrix	twisted	930
uatech	badaso	931
uglifyjs_project	uglifyjs	932
Vestacp	control_panel	932
	vesta_control_panel	933
VIM	vim	933
Vmware	cloud_foundation	934
	nsx_data_center	934
web-based_student_clearance_system_project	web-based_student_clearance_system	935
Webmin	usermin	935
weseek	growi	936
wintercms	winter	936
wire	wire_server	938
wisa	smart_wing_cms	940

Vendor	Product	Page Number
withsecure	f-secure_policy_manager	940
wp_custom_cursors_project	wp_custom_cursors	940
wp_humans.txt_project	wp_humans.txt	942
X.org	libx11	942
	x_server	943
xbifrost	bifrost	944
Yokogawa	wtviewerefree	945
	wtviewere_761941	945
yordam	library_automation_system	946
zalando	skipper	946
Hardware		
Acer	altos_w2000h-w570h_f4	946
Asus	rt-n12e	947
bosch	videojet_multi_4000	947
Cisco	meraki_mx100	948
	meraki_mx105	949
	meraki_mx250	950
	meraki_mx400	951
	meraki_mx450	953
	meraki_mx600	954
	meraki_mx64	955
	meraki_mx64w	956
	meraki_mx65	957
	meraki_mx65w	958
	meraki_mx67	959
	meraki_mx67cw	961
	meraki_mx67w	962
	meraki_mx68	963
	meraki_mx68cw	964
	meraki_mx68w	965
	meraki_mx75	966
	meraki_mx84	967

Vendor	Product	Page Number
Cisco	meraki_mx85	969
	meraki_mx95	970
	meraki_vmx	971
	meraki_z3	972
	meraki_z3c	973
corsair	k63	974
Dlink	dir-816	975
	dir-878	976
gl-inet	gl-ax1800	977
	gl-mt300n-v2	977
Goabode	iota_all-in-one_security_kit	977
gxgroup	gpon_ont_titanium_2122a	984
ip-com	ew9	985
iptime	nas1dual	986
	nas2dual	986
	nas4dual	987
Juniper	acx7100-32c	987
	acx7100-48l	988
	acx7509	990
	csrx	991
	ex2300	991
	ex2300-24mp	993
	ex2300-24p	995
	ex2300-24t	997
	ex2300-48mp	999
	ex2300-48p	1001
	ex2300-48t	1003
	ex2300-c	1005
	ex2300m	1007
	ex3400	1009
	ex4300	1011
	ex4300-24p	1013

Vendor	Product	Page Number
Juniper	ex4300-24p-s	1014
	ex4300-24t	1016
	ex4300-24t-s	1017
	ex4300-32f	1019
	ex4300-32f-dc	1020
	ex4300-32f-s	1022
	ex4300-48mp	1023
	ex4300-48mp-s	1025
	ex4300-48p	1026
	ex4300-48p-s	1028
	ex4300-48t	1029
	ex4300-48t-afi	1031
	ex4300-48t-dc	1032
	ex4300-48t-dc-afi	1034
	ex4300-48t-s	1035
	ex4300-48tafi	1037
	ex4300-48tdc	1038
	ex4300-48tdc-afi	1040
	ex4300-mp	1041
	ex4300-vc	1043
	ex4300m	1044
	ex4600	1046
	ex4600-vc	1047
	ex4650	1049
	mx10	1050
	mx10000	1053
	mx10003	1055
	mx10008	1057
	mx10016	1059
	mx104	1061
	mx150	1064
	mx2008	1066

Vendor	Product	Page Number
Juniper	mx2010	1068
	mx2020	1070
	mx204	1073
	mx240	1075
	mx40	1077
	mx480	1079
	mx5	1081
	mx80	1084
	mx960	1086
	ptx1000	1088
	ptx1000-72q	1090
	ptx10000	1093
	ptx10001	1095
	ptx10001-36mr	1098
	ptx100016	1100
	ptx10002	1102
	ptx10002-60c	1105
	ptx10003	1107
	ptx10003_160c	1109
	ptx10003_80c	1112
	ptx10003_81cd	1114
	ptx10004	1117
	ptx10008	1120
	ptx10016	1123
	ptx3000	1126
	ptx5000	1129
	qfx10002	1131
	qfx10008	1134
	qfx10016	1136
	qfx5100	1138
	qfx5110	1140
	qfx5120	1141

Vendor	Product	Page Number
Juniper	qfx5130	1143
	qfx5200	1144
	qfx5210	1146
	qfx5220	1147
	qfx5700	1149
	srx100	1150
	srx110	1154
	srx1400	1157
	srx1500	1161
	srx210	1165
	srx220	1169
	srx240	1172
	srx240h2	1176
	srx240m	1179
	srx300	1183
	srx320	1187
	srx340	1190
	srx3400	1194
	srx345	1197
	srx3600	1201
	srx380	1205
	srx4000	1208
	srx4100	1213
	srx4200	1218
	srx4600	1223
	srx5000	1229
	srx5400	1233
	srx550	1238
	srx550m	1243
	srx550_hm	1246
	srx5600	1250
	srx5800	1255

Vendor	Product	Page Number
Juniper	srx650	1260
	vsrx	1264
lannerinc	iac-ast2500	1265
	iac-ast2500a	1265
Netgear	r6220	1270
oringnet	iap-420	1270
	iap-420\+	1270
Qualcomm	apq8009	1271
	apq8009w	1274
	apq8016	1276
	apq8017	1277
	apq8037	1280
	apq8052	1281
	apq8053	1284
	apq8056	1286
	apq8064au	1288
	apq8076	1290
	apq8084	1294
	apq8092	1294
	apq8094	1295
	apq8096au	1296
	aqt1000	1299
	ar6003	1304
	ar8031	1305
	ar8035	1308
	ar9380	1312
	csr8811	1314
	csra6620	1316
	csra6640	1320
	csrb31024	1323
	fsm10056	1326
	ipq4018	1327

Vendor	Product	Page Number
Qualcomm	ipq4019	1329
	ipq4028	1329
	ipq4029	1331
	ipq5010	1333
	ipq5018	1336
	ipq5028	1339
	ipq6000	1341
	ipq6010	1343
	ipq6018	1346
	ipq6028	1348
	ipq8064	1351
	ipq8065	1353
	ipq8068	1353
	ipq8069	1354
	ipq8070	1356
	ipq8070a	1358
	ipq8071	1360
	ipq8071a	1362
	ipq8072	1364
	ipq8072a	1366
	ipq8074	1369
	ipq8074a	1370
	ipq8076	1373
	ipq8076a	1375
	ipq8078	1378
	ipq8078a	1380
	ipq8173	1383
	ipq8174	1385
	ipq9008	1388
	kailua	1390
	mdm8215	1390
	mdm8215m	1393

Vendor	Product	Page Number
Qualcomm	mdm8615m	1393
	mdm9150	1394
	mdm9205	1396
	mdm9206	1397
	mdm9215	1399
	mdm9225	1402
	mdm9225m	1402
	mdm9230	1403
	mdm9235m	1404
	mdm9250	1405
	mdm9310	1407
	mdm9330	1410
	mdm9607	1411
	mdm9615	1414
	mdm9615m	1416
	mdm9625	1417
	mdm9625m	1417
	mdm9628	1418
	mdm9630	1421
	mdm9635m	1422
	mdm9640	1423
	mdm9645	1425
	mdm9650	1426
	msm8108	1430
	msm8208	1432
	msm8209	1434
	msm8608	1437
	msm8909w	1439
	msm8917	1441
	msm8920	1443
	msm8937	1444
	msm8940	1445

Vendor	Product	Page Number
Qualcomm	msm8952	1446
	msm8953	1448
	msm8956	1451
	msm8976	1453
	msm8976sg	1456
	msm8992	1459
	msm8994	1459
	msm8996au	1460
	pm8937	1464
	pmp8074	1465
	qam8295p	1467
	qca0000	1472
	qca1023	1473
	qca1062	1474
	qca1064	1476
	qca1990	1478
	qca2062	1479
	qca2064	1481
	qca2065	1483
	qca2066	1485
	qca4004	1487
	qca4010	1488
	qca4020	1489
	qca4024	1492
	qca4531	1495
	qca6164	1496
	qca6174	1497
	qca6174a	1500
	qca6175a	1505
	qca6310	1507
	qca6320	1512
	qca6335	1516

Vendor	Product	Page Number
Qualcomm	qca6390	1521
	qca6391	1526
	qca6420	1532
	qca6421	1537
	qca6426	1541
	qca6428	1546
	qca6430	1547
	qca6431	1552
	qca6436	1557
	qca6438	1561
	qca6554a	1563
	qca6564	1565
	qca6564a	1569
	qca6564au	1574
	qca6574	1580
	qca6574a	1585
	qca6574au	1591
	qca6584	1596
	qca6584au	1599
	qca6595	1602
	qca6595au	1606
	qca6694	1612
	qca6696	1612
	qca7500	1618
	qca8072	1619
	qca8075	1621
	qca8081	1623
	qca8082	1627
	qca8084	1629
	qca8085	1630
	qca8337	1632
	qca8386	1636

Vendor	Product	Page Number
Qualcomm	qca9367	1637
	qca9369	1640
	qca9377	1641
	qca9379	1646
	qca9880	1649
	qca9886	1649
	qca9888	1649
	qca9889	1652
	qca9898	1655
	qca9980	1657
	qca9984	1659
	qca9985	1661
	qca9990	1661
	qca9992	1663
	qca9994	1665
	qcc5100	1667
	qcm2290	1671
	qcm4290	1674
	qcm6125	1676
	qcm6490	1679
	qcn5021	1682
	qcn5022	1684
	qcn5024	1687
	qcn5052	1689
	qcn5054	1692
	qcn5122	1694
	qcn5124	1696
	qcn5152	1699
	qcn5154	1701
	qcn5164	1704
	qcn6023	1706
	qcn6024	1709

Vendor	Product	Page Number
Qualcomm	qcn6100	1712
	qcn6102	1714
	qcn6112	1715
	qcn6122	1717
	qcn6132	1719
	qcn7605	1722
	qcn7606	1724
	qcn9000	1727
	qcn9001	1730
	qcn9002	1731
	qcn9003	1733
	qcn9011	1734
	qcn9012	1736
	qcn9022	1739
	qcn9024	1741
	qcn9070	1744
	qcn9072	1747
	qcn9074	1749
	qcn9100	1752
	qcn9274	1754
	qcs2290	1756
	qcs405	1758
	qcs410	1762
	qcs4290	1766
	qcs603	1768
	qcs605	1771
	qcs610	1775
	qcs6125	1779
	qcs6490	1782
	qcs8155	1785
	qcx315	1786
	qet4101	1788

Vendor	Product	Page Number
Qualcomm	qrb5165	1789
	qrb5165m	1792
	qrb5165n	1794
	qsm8250	1796
	qsm8350	1799
	qsw8573	1801
	qualcomm215	1803
	sa4150p	1805
	sa4155p	1808
	sa415m	1811
	sa515m	1814
	sa6145p	1817
	sa6150p	1823
	sa6155	1828
	sa6155p	1833
	sa8145p	1839
	sa8150p	1844
	sa8155	1850
	sa8155p	1855
	sa8195p	1861
	sa8295p	1866
	sa8540p	1871
	sa9000p	1872
	sc8180x\+sdx55	1873
	sd205	1875
	sd210	1877
	sd429	1880
	sd439	1883
	sd450	1885
	sd460	1887
	sd480	1890
	sd632	1893

Vendor	Product	Page Number
Qualcomm	sd660	1895
	sd662	1898
	sd665	1901
	sd670	1903
	sd675	1906
	sd678	1910
	sd680	1913
	sd690_5g	1916
	sd695	1918
	sd710	1920
	sd712	1923
	sd720g	1925
	sd730	1927
	sd750g	1930
	sd765	1932
	sd765g	1935
	sd768g	1938
	sd778g	1941
	sd780g	1945
	sd7c	1948
	sd820	1950
	sd821	1953
	sd835	1955
	sd845	1959
	sd850	1965
	sd855	1967
	sd865_5g	1972
	sd870	1977
	sd888	1982
	sd888_5g	1985
	sda429w	1989
	sdm429w	1993

Vendor	Product	Page Number
Qualcomm	sdm630	1996
	sdw2500	1998
	sdx12	2000
	sdx20	2002
	sdx20m	2004
	sdx24	2007
	sdx50m	2010
	sdx55	2014
	sdx55m	2019
	sdx57m	2024
	sdx65	2025
	sdxr1	2028
	sdxr2_5g	2031
	sd_455	2035
	sd_636	2038
	sd_675	2040
	sd_8cx	2044
	sd_8cx_gen2	2046
	sd_8cx_gen3	2049
	sd_8_gen1_5g	2051
	sg8275	2057
	sg8275p	2057
	sm4125	2057
	sm4375	2060
	sm6250	2062
	sm6250p	2065
	sm7250p	2067
	sm7315	2070
	sm7325p	2073
	sm8550	2076
	sw5100	2076
	sw5100p	2081

Vendor	Product	Page Number
Qualcomm	sxr2150p	2086
	wcd9306	2088
	wcd9326	2090
	wcd9330	2095
	wcd9335	2097
	wcd9340	2103
	wcd9341	2109
	wcd9360	2115
	wcd9370	2118
	wcd9371	2123
	wcd9375	2125
	wcd9380	2130
	wcd9385	2136
	wcd9390	2141
	wcd9395	2141
	wcn3610	2142
	wcn3615	2146
	wcn3620	2150
	wcn3660	2153
	wcn3660b	2155
	wcn3680	2159
	wcn3680b	2161
	wcn3910	2166
	wcn3950	2168
	wcn3980	2174
	wcn3988	2180
	wcn3990	2184
	wcn3991	2190
	wcn3998	2194
	wcn3999	2200
	wcn6740	2203
	wcn6750	2207

Vendor	Product	Page Number
Qualcomm	wcn6850	2210
	wcn6851	2215
	wcn6855	2220
	wcn6856	2226
	wcn7850	2232
	wcn7851	2237
	wsa8810	2242
	wsa8815	2249
	wsa8830	2255
	wsa8835	2262
	wsa8840	2268
	wsa8845	2268
	wsa8845h	2269
robustel	r1510	2269
Synology	ds3622xs\+	2275
	fs3410	2277
	hd6500	2280
Tenda	11n	2282
	ac10	2282
	ac15	2284
	ac18	2284
	ax1803	2284
	tx3	2285
Tp-link	ax10	2287
	tl-wr841n	2287
Wago	750-8100	2288
	750-8101	2288
	750-8101\/000-010	2289
	750-8101\/025-000	2289
	750-8102	2290
	750-8102\/025-000	2290
	750-8202\/000-011	2291

Vendor	Product	Page Number
Wago	750-8202\/000-012	2291
	750-8202\/000-022	2291
	750-8202\/040-000	2292
	750-8206	2292
	750-8206\/025-000	2293
	750-8206\/025-001	2293
	750-8206\/040-000	2294
	750-8206\/040-001	2294
	750-8207	2295
	750-8207\/025-000	2295
	750-8207\/025-001	2296
	750-8208	2296
	750-8208\/025-000	2297
	750-8208\/025-001	2297
	750-8210	2298
	750-8210\/025-000	2298
	750-8210\/040-000	2298
	750-8211	2299
	750-8211\/040-000	2299
	750-8212	2300
	750-8212\/000-100	2300
	750-8212\/025-000	2301
	750-8212\/025-001	2301
	750-8212\/025-002	2302
	750-8212\/040-000	2302
	750-8212\/040-001	2303
	750-8212\/040-010	2303
	750-8213	2304
	750-8213\/040-010	2304
	750-8214	2305
	750-8215	2305
	750-8216	2306

Vendor	Product	Page Number
Wago	750-8216\/025-000	2306
	750-8216\/025-001	2306
	750-8216\/040-000	2307
	750-8217	2307
	750-8217\/025-000	2308
	750-8217\/600-000	2308
	750-8217\/625-000	2309
	751-9301	2309
	752-8303\/8000-002	2310
	762-4101	2310
	762-4102	2311
	762-4103	2311
	762-4104	2312
	762-4201\/8000-001	2312
	762-4202\/8000-001	2312
	762-4203\/8000-001	2313
	762-4204\/8000-001	2313
	762-4205\/8000-001	2314
	762-4206\/8000-001	2314
	762-4301\/8000-002	2315
	762-4302\/8000-002	2315
	762-4303\/8000-002	2316
	762-4304\/8000-002	2316
	762-5203\/8000-001	2317
	762-5204\/8000-001	2317
	762-5205\/8000-001	2318
	762-5206\/8000-001	2318
	762-5303\/8000-002	2319
	762-5304\/8000-002	2319
	762-5305\/8000-002	2319
	762-5306\/8000-002	2320
	762-6201\/8000-001	2320

Vendor	Product	Page Number
Wago	762-6202\/8000-001	2321
	762-6203\/8000-001	2321
	762-6204\/8000-001	2322
	762-6301\/8000-002	2322
	762-6302\/8000-002	2323
	762-6303\/8000-002	2323
	762-6304\/8000-002	2324
Operating System		
Acer	altos_w2000h-w570h_f4_firmware	2324
Apple	macos	2325
Asus	rt-n12e_firmware	2326
bosch	videojet_multi_4000_firmware	2327
Broadcom	fabric_operating_system	2327
Cisco	meraki_mx100_firmware	2339
	meraki_mx105_firmware	2341
	meraki_mx250_firmware	2343
	meraki_mx400_firmware	2346
	meraki_mx450_firmware	2348
	meraki_mx600_firmware	2350
	meraki_mx64w_firmware	2352
	meraki_mx64_firmware	2355
	meraki_mx65w_firmware	2357
	meraki_mx65_firmware	2359
	meraki_mx67cw_firmware	2361
	meraki_mx67w_firmware	2364
	meraki_mx67_firmware	2366
	meraki_mx68cw_firmware	2368
	meraki_mx68w_firmware	2370
	meraki_mx68_firmware	2373
	meraki_mx75_firmware	2375
	meraki_mx84_firmware	2377
	meraki_mx85_firmware	2379

Vendor	Product	Page Number
Cisco	meraki_mx95_firmware	2382
	meraki_vmx_firmware	2384
	meraki_z3c_firmware	2386
	meraki_z3_firmware	2387
	roomos	2388
corsair	k63_firmware	2391
Dell	emc_powerscale_onefs	2391
	powerstoreos	2396
Dlink	dir-816_firmware	2397
	dir-878_firmware	2398
F5	f5os-a	2399
	f5os-c	2399
Fedoraproject	fedora	2400
Fortinet	fortios	2401
gl-inet	gl-ax1800_firmware	2404
	gl-mt300n-v2_firmware	2404
Goabode	iota_all-in-one_security_kit_firmware	2405
gxgroup	gpon_ont_titanium_2122a_firmware	2441
ip-com	ew9_firmware	2442
iptime	nas1dual_firmware	2443
	nas2dual_firmware	2443
	nas4dual_firmware	2444
Juniper	junos	2444
	junos_os_evolved	2782
lannerinc	iac-ast2500a_firmware	2884
	iac-ast2500_firmware	2888
Linux	linux_kernel	2888
Microsoft	windows	2910
Netapp	clustered_data_ontap	2912
Netgear	r6220_firmware	2912
Oracle	solaris	2913
oringnet	iap-420\+_firmware	2915

Vendor	Product	Page Number
oringnet	iap-420_firmware	2915
Qualcomm	apq8009w_firmware	2916
	apq8009_firmware	2918
	apq8016_firmware	2921
	apq8017_firmware	2922
	apq8037_firmware	2925
	apq8052_firmware	2926
	apq8053_firmware	2929
	apq8056_firmware	2931
	apq8064au_firmware	2933
	apq8076_firmware	2935
	apq8084_firmware	2939
	apq8092_firmware	2939
	apq8094_firmware	2940
	apq8096au_firmware	2940
	aqt1000_firmware	2944
	ar6003_firmware	2949
	ar8031_firmware	2950
	ar8035_firmware	2953
	ar9380_firmware	2956
	csr8811_firmware	2958
	csra6620_firmware	2961
	csra6640_firmware	2965
	csrb31024_firmware	2968
	fsm10056_firmware	2971
	ipq4018_firmware	2972
	ipq4019_firmware	2974
	ipq4028_firmware	2974
	ipq4029_firmware	2976
	ipq5010_firmware	2978
	ipq5018_firmware	2981
	ipq5028_firmware	2984

Vendor	Product	Page Number
Qualcomm	ipq6000_firmware	2986
	ipq6010_firmware	2988
	ipq6018_firmware	2991
	ipq6028_firmware	2993
	ipq8064_firmware	2996
	ipq8065_firmware	2998
	ipq8068_firmware	2998
	ipq8069_firmware	2999
	ipq8070a_firmware	3001
	ipq8070_firmware	3003
	ipq8071a_firmware	3005
	ipq8071_firmware	3008
	ipq8072a_firmware	3009
	ipq8072_firmware	3012
	ipq8074a_firmware	3013
	ipq8074_firmware	3016
	ipq8076a_firmware	3018
	ipq8076_firmware	3020
	ipq8078a_firmware	3023
	ipq8078_firmware	3025
	ipq8173_firmware	3028
	ipq8174_firmware	3030
	ipq9008_firmware	3033
	kailua_firmware	3035
	mdm8215m_firmware	3035
	mdm8215_firmware	3035
	mdm8615m_firmware	3038
	mdm9150_firmware	3039
	mdm9205_firmware	3041
	mdm9206_firmware	3042
	mdm9215_firmware	3044
	mdm9225m_firmware	3047

Vendor	Product	Page Number
Qualcomm	mdm9225_firmware	3047
	mdm9230_firmware	3048
	mdm9235m_firmware	3049
	mdm9250_firmware	3050
	mdm9310_firmware	3052
	mdm9330_firmware	3055
	mdm9607_firmware	3056
	mdm9615m_firmware	3059
	mdm9615_firmware	3059
	mdm9625m_firmware	3062
	mdm9625_firmware	3062
	mdm9628_firmware	3063
	mdm9630_firmware	3066
	mdm9635m_firmware	3067
	mdm9640_firmware	3068
	mdm9645_firmware	3070
	mdm9650_firmware	3071
	msm8108_firmware	3075
	msm8208_firmware	3077
	msm8209_firmware	3079
	msm8608_firmware	3082
	msm8909w_firmware	3084
	msm8917_firmware	3086
	msm8920_firmware	3088
	msm8937_firmware	3089
	msm8940_firmware	3090
	msm8952_firmware	3091
	msm8953_firmware	3093
	msm8956_firmware	3096
	msm8976sg_firmware	3098
	msm8976_firmware	3100
	msm8992_firmware	3104

Vendor	Product	Page Number
Qualcomm	msm8994_firmware	3104
	msm8996au_firmware	3105
	pm8937_firmware	3109
	pmp8074_firmware	3110
	qam8295p_firmware	3112
	qca0000_firmware	3116
	qca1023_firmware	3118
	qca1062_firmware	3119
	qca1064_firmware	3121
	qca1990_firmware	3123
	qca2062_firmware	3124
	qca2064_firmware	3126
	qca2065_firmware	3128
	qca2066_firmware	3130
	qca4004_firmware	3132
	qca4010_firmware	3133
	qca4020_firmware	3134
	qca4024_firmware	3137
	qca4531_firmware	3140
	qca6164_firmware	3141
	qca6174a_firmware	3142
	qca6174_firmware	3147
	qca6175a_firmware	3150
	qca6310_firmware	3152
	qca6320_firmware	3157
	qca6335_firmware	3161
	qca6390_firmware	3166
	qca6391_firmware	3171
	qca6420_firmware	3177
	qca6421_firmware	3182
	qca6426_firmware	3186
	qca6428_firmware	3191

Vendor	Product	Page Number
Qualcomm	qca6430_firmware	3192
	qca6431_firmware	3197
	qca6436_firmware	3202
	qca6438_firmware	3206
	qca6554a_firmware	3208
	qca6564au_firmware	3210
	qca6564a_firmware	3216
	qca6564_firmware	3221
	qca6574au_firmware	3225
	qca6574a_firmware	3231
	qca6574_firmware	3236
	qca6584au_firmware	3242
	qca6584_firmware	3245
	qca6595au_firmware	3247
	qca6595_firmware	3253
	qca6694_firmware	3257
	qca6696_firmware	3258
	qca7500_firmware	3263
	qca8072_firmware	3264
	qca8075_firmware	3266
	qca8081_firmware	3268
	qca8082_firmware	3272
	qca8084_firmware	3274
	qca8085_firmware	3275
	qca8337_firmware	3277
	qca8386_firmware	3281
	qca9367_firmware	3283
	qca9369_firmware	3285
	qca9377_firmware	3286
	qca9379_firmware	3291
	qca9880_firmware	3294
	qca9886_firmware	3294

Vendor	Product	Page Number
Qualcomm	qca9888_firmware	3295
	qca9889_firmware	3297
	qca9898_firmware	3300
	qca9980_firmware	3302
	qca9984_firmware	3304
	qca9985_firmware	3306
	qca9990_firmware	3306
	qca9992_firmware	3308
	qca9994_firmware	3310
	qcc5100_firmware	3312
	qcm2290_firmware	3317
	qcm4290_firmware	3319
	qcm6125_firmware	3321
	qcm6490_firmware	3324
	qcn5021_firmware	3327
	qcn5022_firmware	3329
	qcn5024_firmware	3332
	qcn5052_firmware	3334
	qcn5054_firmware	3337
	qcn5122_firmware	3339
	qcn5124_firmware	3342
	qcn5152_firmware	3344
	qcn5154_firmware	3347
	qcn5164_firmware	3349
	qcn6023_firmware	3352
	qcn6024_firmware	3354
	qcn6100_firmware	3357
	qcn6102_firmware	3359
	qcn6112_firmware	3360
	qcn6122_firmware	3362
	qcn6132_firmware	3365
	qcn7605_firmware	3367

Vendor	Product	Page Number
Qualcomm	qcn7606_firmware	3369
	qcn9000_firmware	3372
	qcn9001_firmware	3375
	qcn9002_firmware	3376
	qcn9003_firmware	3378
	qcn9011_firmware	3379
	qcn9012_firmware	3381
	qcn9022_firmware	3384
	qcn9024_firmware	3386
	qcn9070_firmware	3389
	qcn9072_firmware	3392
	qcn9074_firmware	3394
	qcn9100_firmware	3397
	qcn9274_firmware	3399
	qcs2290_firmware	3401
	qcs405_firmware	3403
	qcs410_firmware	3407
	qcs4290_firmware	3411
	qcs603_firmware	3413
	qcs605_firmware	3416
	qcs610_firmware	3420
	qcs6125_firmware	3424
	qcs6490_firmware	3427
	qcs8155_firmware	3430
	qcx315_firmware	3431
	qet4101_firmware	3433
	qrb5165m_firmware	3434
	qrb5165n_firmware	3437
	qrb5165_firmware	3439
	qsm8250_firmware	3441
	qsm8350_firmware	3444
	qsw8573_firmware	3446

Vendor	Product	Page Number
Qualcomm	qualcomm215_firmware	3448
	sa4150p_firmware	3450
	sa4155p_firmware	3453
	sa415m_firmware	3456
	sa515m_firmware	3459
	sa6145p_firmware	3462
	sa6150p_firmware	3468
	sa6155p_firmware	3473
	sa6155_firmware	3479
	sa8145p_firmware	3484
	sa8150p_firmware	3489
	sa8155p_firmware	3495
	sa8155_firmware	3501
	sa8195p_firmware	3506
	sa8295p_firmware	3511
	sa8540p_firmware	3516
	sa9000p_firmware	3517
	sc8180x\+sdx55_firmware	3518
	sd205_firmware	3520
	sd210_firmware	3522
	sd429_firmware	3525
	sd439_firmware	3528
	sd450_firmware	3530
	sd460_firmware	3532
	sd480_firmware	3535
	sd632_firmware	3538
	sd660_firmware	3540
	sd662_firmware	3543
	sd665_firmware	3546
	sd670_firmware	3548
	sd675_firmware	3551
	sd678_firmware	3555

Vendor	Product	Page Number
Qualcomm	sd680_firmware	3558
	sd690_5g_firmware	3561
	sd695_firmware	3563
	sd710_firmware	3565
	sd712_firmware	3568
	sd720g_firmware	3570
	sd730_firmware	3572
	sd750g_firmware	3575
	sd765g_firmware	3577
	sd765_firmware	3580
	sd768g_firmware	3583
	sd778g_firmware	3586
	sd780g_firmware	3590
	sd7c_firmware	3593
	sd820_firmware	3595
	sd821_firmware	3598
	sd835_firmware	3600
	sd845_firmware	3604
	sd850_firmware	3610
	sd855_firmware	3612
	sd865_5g_firmware	3617
	sd870_firmware	3622
	sd888_5g_firmware	3627
	sd888_firmware	3631
	sda429w_firmware	3634
	sdm429w_firmware	3638
	sdm630_firmware	3641
	sdw2500_firmware	3643
	sdx12_firmware	3645
	sdx20m_firmware	3647
	sdx20_firmware	3649
	sdx24_firmware	3652

Vendor	Product	Page Number
Qualcomm	sdx50m_firmware	3655
	sdx55m_firmware	3659
	sdx55_firmware	3664
	sdx57m_firmware	3669
	sdx65_firmware	3670
	sdxr1_firmware	3673
	sdxr2_5g_firmware	3676
	sd_455_firmware	3680
	sd_636_firmware	3683
	sd_675_firmware	3685
	sd_8cx_firmware	3689
	sd_8cx_gen2_firmware	3691
	sd_8cx_gen3_firmware	3694
	sd_8_gen1_5g_firmware	3696
	sg8275p_firmware	3701
	sg8275_firmware	3702
	sm4125_firmware	3702
	sm4375_firmware	3705
	sm6250p_firmware	3707
	sm6250_firmware	3709
	sm7250p_firmware	3712
	sm7315_firmware	3715
	sm7325p_firmware	3718
	sm8550_firmware	3721
	sw5100p_firmware	3721
	sw5100_firmware	3726
	sxr2150p_firmware	3731
	wcd9306_firmware	3733
	wcd9326_firmware	3735
	wcd9330_firmware	3740
	wcd9335_firmware	3742
	wcd9340_firmware	3748

Vendor	Product	Page Number
Qualcomm	wcd9341_firmware	3754
	wcd9360_firmware	3760
	wcd9370_firmware	3763
	wcd9371_firmware	3768
	wcd9375_firmware	3770
	wcd9380_firmware	3775
	wcd9385_firmware	3781
	wcd9390_firmware	3786
	wcd9395_firmware	3786
	wcn3610_firmware	3787
	wcn3615_firmware	3791
	wcn3620_firmware	3795
	wcn3660b_firmware	3798
	wcn3660_firmware	3802
	wcn3680b_firmware	3804
	wcn3680_firmware	3809
	wcn3910_firmware	3811
	wcn3950_firmware	3814
	wcn3980_firmware	3819
	wcn3988_firmware	3825
	wcn3990_firmware	3829
	wcn3991_firmware	3835
	wcn3998_firmware	3839
	wcn3999_firmware	3845
	wcn6740_firmware	3848
	wcn6750_firmware	3852
	wcn6850_firmware	3855
	wcn6851_firmware	3860
	wcn6855_firmware	3865
	wcn6856_firmware	3871
	wcn7850_firmware	3877
	wcn7851_firmware	3882

Vendor	Product	Page Number
Qualcomm	wsa8810_firmware	-
	wsa8815_firmware	3894
	wsa8830_firmware	3900
	wsa8835_firmware	3907
	wsa8840_firmware	3913
	wsa8845h_firmware	3913
	wsa8845_firmware	3914
robustel	r1510_firmware	3914
Tenda	11n_firmware	3926
	ac10_firmware	3927
	ac15_firmware	3929
	ac18_firmware	3929
	ax1803_firmware	3929
	tx3_firmware	3930
Tp-link	ax10_firmware	3932
	tl-wr841n_firmware	3932
Wago	750-8100_firmware	3933
	750-8101\/000-010_firmware	3933
	750-8101\/025-000_firmware	3934
	750-8101_firmware	3934
	750-8102\/025-000_firmware	3935
	750-8102_firmware	3935
	750-8202\/000-011_firmware	3936
	750-8202\/000-012_firmware	3936
	750-8202\/000-022_firmware	3937
	750-8202\/040-000_firmware	3937
	750-8206\/025-000_firmware	3937
	750-8206\/025-001_firmware	3938
	750-8206\/040-000_firmware	3938
	750-8206\/040-001_firmware	3939
	750-8206_firmware	3939
	750-8207\/025-000_firmware	3940

Vendor	Product	Page Number
Wago	750-8207\/025-001_firmware	3940
	750-8207_firmware	3941
	750-8208\/025-000_firmware	3941
	750-8208\/025-001_firmware	3942
	750-8208_firmware	3942
	750-8210\/025-000_firmware	3943
	750-8210\/040-000_firmware	3943
	750-8210_firmware	3944
	750-8211\/040-000_firmware	3944
	750-8211_firmware	3944
	750-8212\/000-100_firmware	3945
	750-8212\/025-000_firmware	3945
	750-8212\/025-001_firmware	3946
	750-8212\/025-002_firmware	3946
	750-8212\/040-000_firmware	3947
	750-8212\/040-001_firmware	3947
	750-8212\/040-010_firmware	3948
	750-8212_firmware	3948
	750-8213\/040-010_firmware	3949
	750-8213_firmware	3949
	750-8214_firmware	3950
	750-8215_firmware	3950
	750-8216\/025-000_firmware	3951
	750-8216\/025-001_firmware	3951
	750-8216\/040-000_firmware	3951
	750-8216_firmware	3952
	750-8217\/025-000_firmware	3952
	750-8217\/600-000_firmware	3953
	750-8217\/625-000_firmware	3953
	750-8217_firmware	3954
	751-9301_firmware	3954
	752-8303\/8000-002_firmware	3955

Vendor	Product	Page Number
Wago	762-4101_firmware	3955
	762-4102_firmware	3956
	762-4103_firmware	3956
	762-4104_firmware	3957
	762-4201\/8000-001_firmware	3957
	762-4202\/8000-001_firmware	3958
	762-4203\/8000-001_firmware	3958
	762-4204\/8000-001_firmware	3958
	762-4205\/8000-001_firmware	3959
	762-4206\/8000-001_firmware	3959
	762-4301\/8000-002_firmware	3960
	762-4302\/8000-002_firmware	3960
	762-4303\/8000-002_firmware	3961
	762-4304\/8000-002_firmware	3961
	762-5203\/8000-001_firmware	3962
	762-5204\/8000-001_firmware	3962
	762-5205\/8000-001_firmware	3963
	762-5206\/8000-001_firmware	3963
	762-5303\/8000-002_firmware	3964
	762-5304\/8000-002_firmware	3964
	762-5305\/8000-002_firmware	3965
	762-5306\/8000-002_firmware	3965
	762-6201\/8000-001_firmware	3965
	762-6202\/8000-001_firmware	3966
	762-6203\/8000-001_firmware	3966
	762-6204\/8000-001_firmware	3967
	762-6301\/8000-002_firmware	3967
	762-6302\/8000-002_firmware	3968
	762-6303\/8000-002_firmware	3968
	762-6304\/8000-002_firmware	3969

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 10web					
Product: form_maker					
Affected Version(s): * Up to (excluding) 1.15.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2022	7.2	The Form Maker by 10Web WordPress plugin before 1.15.6 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin **CVE ID : CVE-2022-3300**	https://wpscan.com/vulnerability/ddc9ed69-d942-4fad-bbf4-1be3b86460d9	A-10W-FORM-041122/1
Vendor: 74cms					
Product: 74cmsse					
Affected Version(s): 3.12.0					
Incorrect Permission Assignment for Critical Resource	17-Oct-2022	6.5	74cmsSE v3.12.0 allows authenticated attackers with low-level privileges to arbitrarily change the rights and credentials of the Super Administrator account. **CVE ID : CVE-2022-41471**	N/A	A-74C-74CM-041122/2
Improper Neutralization of Input During Web Page Generation ('Cross-site	17-Oct-2022	5.4	74cmsSE v3.12.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /apiadmin/notice/add. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted	N/A	A-74C-74CM-041122/3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			payload injected into the Title field. **CVE ID : CVE-2022-41472**		
Affected Version(s): 3.13.0					
Unrestricted Upload of File with Dangerous Type	17-Oct-2022	9.8	An arbitrary file upload vulnerability in the component /apiadmin/upload/attach of 74cmsSE v3.13.0 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-42154**	N/A	A-74C-74CM-041122/4
Vendor: abpressoptimizer					
Product: ab_press_optimizer					
Affected Version(s): * Up to (including) 1.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Mammothology AB Press Optimizer plugin <= 1.1.1 on WordPress. **CVE ID : CVE-2022-26375**	https://patchstack.com/database/vulnerability/ab-press-optimizer-lite/wordpress-ab-press-optimizer-plugin-1-1-1-auth-stored-cross-site-scripting-xss-vulnerability?_s_id=cve, https://wordpress.org/plugins/ab-press-	A-ABP-AB_P-041122/5

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				optimizer-lite/	
Vendor: adenion					
Product: blog2social					
Affected Version(s): * Up to (excluding) 6.9.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2022	8.8	The Blog2Social: Social Media Auto Post & Scheduler WordPress plugin before 6.9.10 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by any authenticated users, such as subscribers **CVE ID : CVE-2022-3246**	https://wpscan.com/vulnerability/ece049b2-9a21-463d-9e8b-b4ce61919f0c	A-ADE-BLOG-041122/6
Server-Side Request Forgery (SSRF)	25-Oct-2022	6.5	The Blog2Social: Social Media Auto Post & Scheduler WordPress plugin before 6.9.10 does not have authorisation in an AJAX action, and does not ensure that the URL to make a request to is an external one. As a result, any authenticated users, such as subscriber could perform SSRF attacks **CVE ID : CVE-2022-3247**	https://wpscan.com/vulnerability/ee312f22-ca58-451d-a1cb-3f78a6e5ecaf	A-ADE-BLOG-041122/7
Vendor: adminpad_project					
Product: adminpad					
Affected Version(s): * Up to (excluding) 2.2					
Cross-Site Request Forgery (CSRF)	25-Oct-2022	6.5	The AdminPad WordPress plugin before 2.2 does not have CSRF check when updating	N/A	A-ADM-ADMI-041122/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin's note, allowing attackers to make a logged in admin update their notes via a CSRF attack **CVE ID : CVE-2022-2762**		
Vendor: Adobe					
Product: commerce					
Affected Version(s): * Up to (excluding) 2.3.7					
Improper Input Validation	20-Oct-2022	8.8	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an improper input validation vulnerability. An authenticated attacker can trigger an insecure direct object reference in the `V1/customers/me` endpoint to achieve information exposure and privilege escalation. **CVE ID : CVE-2022-42344**	https://helpx.adobe.com/security/products/magento/apsb22-38.html	A-ADO-COMM-041122/9
Affected Version(s): 2.3.7					
Improper Input Validation	20-Oct-2022	8.8	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an improper input validation vulnerability. An authenticated attacker can trigger an insecure direct object reference in the `V1/customers/me` endpoint to achieve	https://helpx.adobe.com/security/products/magento/apsb22-38.html	A-ADO-COMM-041122/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information exposure and privilege escalation. **CVE ID : CVE-2022-42344**		
Affected Version(s): 2.4.3					
Improper Input Validation	20-Oct-2022	8.8	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an improper input validation vulnerability. An authenticated attacker can trigger an insecure direct object reference in the `V1/customers/me` endpoint to achieve information exposure and privilege escalation. **CVE ID : CVE-2022-42344**	https://helpx.adobe.com/security/products/magento/apsb22-38.html	A-ADO-COMM-041122/11
Affected Version(s): 2.4.4					
Improper Input Validation	20-Oct-2022	8.8	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an improper input validation vulnerability. An authenticated attacker can trigger an insecure direct object reference in the `V1/customers/me` endpoint to achieve information exposure and privilege escalation. **CVE ID : CVE-2022-42344**	https://helpx.adobe.com/security/products/magento/apsb22-38.html	A-ADO-COMM-041122/12
Affected Version(s): From (including) 2.4.0 Up to (excluding) 2.4.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Oct-2022	8.8	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an improper input validation vulnerability. An authenticated attacker can trigger an insecure direct object reference in the `V1/customers/me` endpoint to achieve information exposure and privilege escalation. **CVE ID : CVE-2022-42344**	https://helpx.adobe.com/security/products/magento/apsb22-38.html	A-ADO-COMM-041122/13
Product: illustrator					
Affected Version(s): * Up to (including) 25.4.7					
Out-of-bounds Read	25-Oct-2022	7.8	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38436**	https://helpx.adobe.com/security/products/illustrator/apsb22-56.html	A-ADO-ILLU-041122/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	25-Oct-2022	7.8	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38435**	https://helpx.adobe.com/security/products/illustrator/apsb22-56.html	A-ADO-ILLU-041122/15
Affected Version(s): From (including) 26.0 Up to (including) 26.4					
Out-of-bounds Read	25-Oct-2022	7.8	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38436**	https://helpx.adobe.com/security/products/illustrator/apsb22-56.html	A-ADO-ILLU-041122/16
Improper Input Validation	25-Oct-2022	7.8	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by	https://helpx.adobe.com/security/products/illust	A-ADO-ILLU-041122/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38435**	rator/apsb22-56.html	
Vendor: Advantech					
Product: r-seenet					
Affected Version(s): * Up to (including) 2.4.17					
Out-of-bounds Write	27-Oct-2022	9.8	Advantech R-SeeNet Versions 2.4.17 and prior are vulnerable to a stack-based buffer overflow. An unauthorized attacker can remotely overflow the stack buffer and enable remote code execution. **CVE ID : CVE-2022-3385**	N/A	A-ADV-R-SE-041122/18
Out-of-bounds Write	27-Oct-2022	9.8	Advantech R-SeeNet Versions 2.4.17 and prior are vulnerable to a stack-based buffer overflow. An unauthorized attacker can use an outsized filename to overflow the stack buffer and enable remote code execution. **CVE ID : CVE-2022-3386**	N/A	A-ADV-R-SE-041122/19
Affected Version(s): * Up to (including) 2.4.19					
Improper Limitation of a	27-Oct-2022	5.3	Advantech R-SeeNet Versions 2.4.19 and prior are vulnerable to path	N/A	A-ADV-R-SE-041122/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			traversal attacks. An unauthorized attacker could remotely exploit vulnerable PHP code to delete .PDF files. **CVE ID : CVE-2022-3387**		
Vendor: aethon					
Product: tug_home_base_server					
Affected Version(s): * Up to (excluding) 24					
Missing Authorization	21-Oct-2022	8.2	Aethon TUG Home Base Server versions prior to version 24 are affected by un unauthenticated attacker who can freely access hashed user credentials. **CVE ID : CVE-2022-1066**	N/A	A-AET-TUG_-041122/21
N/A	21-Oct-2022	8.1	Aethon TUG Home Base Server versions prior to version 24 are affected by un unauthenticated attacker who can freely access hashed user credentials. **CVE ID : CVE-2022-1070**	N/A	A-AET-TUG_-041122/22
Missing Authorization	21-Oct-2022	7.5	Aethon TUG Home Base Server versions prior to version 24 are affected by un unauthenticated attacker who can freely access hashed user credentials. **CVE ID : CVE-2022-26423**	N/A	A-AET-TUG_-041122/23
Improper Neutralization of	21-Oct-2022	6.1	Aethon TUG Home Base Server versions prior to version 24 are affected	N/A	A-AET-TUG_-041122/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			by un unauthenticated attacker who can freely access hashed user credentials. **CVE ID : CVE-2022-1059**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-2022	5.4	Aethon TUG Home Base Server versions prior to version 24 are affected by un unauthenticated attacker who can freely access hashed user credentials. **CVE ID : CVE-2022-27494**	N/A	A-AET-TUG_-041122/25
Vendor: Algosec					
Product: fireflow					
Affected Version(s): From (including) a32.0 Up to (excluding) a32.0.580-277					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2022	5.4	AlgoSec – FireFlow Reflected Cross-Site-Scripting (RXSS) A malicious user injects JavaScript code into a parameter called IntersectudRule on the search/result.html page. The malicious user changes the request from POST to GET and sends the URL to another user (victim). JavaScript code is executed on the browser of the other user. **CVE ID : CVE-2022-36783**	N/A	A-ALG-FIRE-041122/26
Affected Version(s): From (including) a32.10 Up to (excluding) a32.10.410-212					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2022	5.4	AlgoSec – FireFlow Reflected Cross-Site-Scripting (RXSS) A malicious user injects JavaScript code into a parameter called IntersectudRule on the search/result.html page. The malicious user changes the request from POST to GET and sends the URL to another user (victim). JavaScript code is executed on the browser of the other user. **CVE ID : CVE-2022-36783**	N/A	A-ALG-FIRE-041122/27
Affected Version(s): From (including) a32.20 Up to (excluding) a32.20.230-35					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2022	5.4	AlgoSec – FireFlow Reflected Cross-Site-Scripting (RXSS) A malicious user injects JavaScript code into a parameter called IntersectudRule on the search/result.html page. The malicious user changes the request from POST to GET and sends the URL to another user (victim). JavaScript code is executed on the browser of the other user. **CVE ID : CVE-2022-36783**	N/A	A-ALG-FIRE-041122/28
Vendor: alivecor					
Product: kardia					
Affected Version(s): * Up to (including) 5.17.1-754993421					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	26-Oct-2022	6.1	CWE-302 Authentication Bypass by Assumed-Immutable Data in AliveCor Kardia App version 5.17.1-754993421 and prior on Android allows an unauthenticated attacker with physical access to the Android device containing the app to bypass application authentication and alter information in the app. **CVE ID : CVE-2022-40703**	N/A	A-ALI-KARD-041122/29
Vendor: anji-plus					
Product: report					
Affected Version(s): 0.9.8.6					
Authentication Bypass by Spoofing	17-Oct-2022	8.8	anji-plus AJ-Report 0.9.8.6 allows remote attackers to bypass login authentication by spoofing JWT Tokens. **CVE ID : CVE-2022-42983**	N/A	A-ANJ-REPO-041122/30
Vendor: Apache					
Product: batik					
Affected Version(s): From (including) 1.0 Up to (excluding) 1.16					
Server-Side Request Forgery (SSRF)	25-Oct-2022	7.5	A vulnerability in Batik of Apache XML Graphics allows an attacker to run untrusted Java code from an SVG. This issue affects Apache XML Graphics prior to 1.16. It is recommended to update to version 1.16. **CVE ID : CVE-2022-41704**	https://lists.apache.org/thread/hplhx0o74jb7blj39fm4kw3otcnjd6xf	A-APA-BATI-041122/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	25-Oct-2022	7.5	A vulnerability in Batik of Apache XML Graphics allows an attacker to run Java code from untrusted SVG via JavaScript. This issue affects Apache XML Graphics prior to 1.16. Users are recommended to upgrade to version 1.16. **CVE ID : CVE-2022-42890**	https://lists.apache.org/thread/pkvhy0nsj1h1mlon008wtzhosbtxjwly	A-APA-BATI-041122/32
Product: dolphinscheduler					
Affected Version(s): * Up to (excluding) 2.0.6					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Oct-2022	6.5	Users can read any files by log server, Apache DolphinScheduler users should upgrade to version 2.0.6 or higher. **CVE ID : CVE-2022-26884**	https://lists.apache.org/thread/xfdst5y4hnrm2ntmc5jzrgmw2htyyb9c	A-APA-DOLP-041122/33
Product: dubbo					
Affected Version(s): 3.1.0					
Deserialization of Untrusted Data	18-Oct-2022	9.8	A deserialization vulnerability existed in dubbo hessian-lite 3.2.12 and its earlier versions, which could lead to malicious code execution. This issue affects Apache Dubbo 2.7.x version 2.7.17 and prior versions; Apache Dubbo 3.0.x version 3.0.11 and prior versions; Apache Dubbo 3.1.x version 3.1.0 and prior versions.	https://lists.apache.org/thread/8d3zqrkoy4jh8dy37j4rd7g9jodzlvkk	A-APA-DUBB-041122/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39198		
Affected Version(s): From (including) 2.7.0 Up to (including) 2.7.17					
Deserialization of Untrusted Data	18-Oct-2022	9.8	A deserialization vulnerability existed in dubbo hessian-lite 3.2.12 and its earlier versions, which could lead to malicious code execution. This issue affects Apache Dubbo 2.7.x version 2.7.17 and prior versions; Apache Dubbo 3.0.x version 3.0.11 and prior versions; Apache Dubbo 3.1.x version 3.1.0 and prior versions. **CVE ID : CVE-2022-39198**	https://lists.apache.org/thread/8d3zqrkoy4jh8dy37j4rd7g9jodzlvkk	A-APA-DUBB-041122/35
Affected Version(s): From (including) 3.0.0 Up to (including) 3.0.11					
Deserialization of Untrusted Data	18-Oct-2022	9.8	A deserialization vulnerability existed in dubbo hessian-lite 3.2.12 and its earlier versions, which could lead to malicious code execution. This issue affects Apache Dubbo 2.7.x version 2.7.17 and prior versions; Apache Dubbo 3.0.x version 3.0.11 and prior versions; Apache Dubbo 3.1.x version 3.1.0 and prior versions. **CVE ID : CVE-2022-39198**	https://lists.apache.org/thread/8d3zqrkoy4jh8dy37j4rd7g9jodzlvkk	A-APA-DUBB-041122/36
Product: flume					
Affected Version(s): From (including) 1.4.0 Up to (including) 1.10.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	26-Oct-2022	9.8	Apache Flume versions 1.4.0 through 1.10.1 are vulnerable to a remote code execution (RCE) attack when a configuration uses a JMS Source with an unsafe providerURL. This issue is fixed by limiting JNDI to allow only the use of the java protocol or no protocol. **CVE ID : CVE-2022-42468**	https://lists.apache.org/thread/939wkx8o90bp6m2ht3t1sdyo1ncypl78, https://lists.apache.org/thread/1ckhmp539zr2nd2rs45pocpywk2d9zvz, https://issues.apache.org/jira/browse/FLUME-3437	A-APA-FLUM-041122/37
Product: geode					
Affected Version(s): * Up to (including) 1.15.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2022	5.4	Apache Geode versions up to 1.15.0 are vulnerable to a Cross-Site Scripting (XSS) via data injection when using Pulse web application to view Region entries. **CVE ID : CVE-2022-34870**	https://lists.apache.org/thread/zltlr7f2ymr2m6jj54k4z0c4foos5fwx	A-APA-GEOD-041122/38
Product: heron					
Affected Version(s): * Up to (excluding) 0.20.5-incubating					
Improper Neutralization of Special Elements in Output Used by a Downstream Compone	24-Oct-2022	9.8	Heron versions <= 0.20.4-incubating allows CRLF log injection because of the lack of escaping in the log statements. Please update to version 0.20.5-incubating which addresses this issue.	https://lists.apache.org/thread/j65nwr8n7jchngwqptzh100drcr4ry2q	A-APA-HERO-041122/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
nt ('Injection')			**CVE ID : CVE-2021-42010**		
Product: iotdb					
Affected Version(s): From (including) 0.12.2 Up to (including) 0.12.6					
N/A	26-Oct-2022	7.5	Apache IoTDB version 0.12.2 to 0.12.6, 0.13.0 to 0.13.2 are vulnerable to a Denial of Service attack when accepting untrusted patterns for REGEXP queries with Java 8. Users should upgrade to 0.13.3 which addresses this issue or use a later version of Java to avoid it. **CVE ID : CVE-2022-43766**	https://lists.apache.org/thread/9pgpb82p5brooy41n8l5q0y9h33db2zn	A-APA-IOTD-041122/40
Affected Version(s): From (including) 0.13.0 Up to (including) 0.13.2					
N/A	26-Oct-2022	7.5	Apache IoTDB version 0.12.2 to 0.12.6, 0.13.0 to 0.13.2 are vulnerable to a Denial of Service attack when accepting untrusted patterns for REGEXP queries with Java 8. Users should upgrade to 0.13.3 which addresses this issue or use a later version of Java to avoid it. **CVE ID : CVE-2022-43766**	https://lists.apache.org/thread/9pgpb82p5brooy41n8l5q0y9h33db2zn	A-APA-IOTD-041122/41
Product: isis					
Affected Version(s): * Up to (excluding) 2.0.0					
Improper Neutralization of Input During	19-Oct-2022	6.1	Prior to 2.0.0-M9, it was possible for an end-user to set the value of an editable string property of a domain object to a	https://lists.apache.org/thread/83ftj5jgtv3mbm28	A-APA-ISIS-041122/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			value that would be rendered unchanged when the value was saved. In particular, the end-user could enter javascript or similar and this would be executed. As of this release, the inputted strings are properly escaped when rendered. **CVE ID : CVE-2022-42466**	w3trjyvd591jztrz	
Insecure Default Initialization of Resource	19-Oct-2022	5.3	When running in prototype mode, the h2 webconsole module (accessible from the Prototype menu) is automatically made available with the ability to directly query the database. It was felt that it is safer to require the developer to explicitly enable this capability. As of 2.0.0-M8, this can now be done using the 'isis.prototyping.h2-console.web-allow-remote-access' configuration property; the web console will be unavailable without setting this configuration. As an additional safeguard, the new 'isis.prototyping.h2-console.generate-random-web-admin-password' configuration parameter (enabled by default) requires that the administrator use a	https://lists.apache.org/thread/jbv2ddt00h7ntlbm6vkk4wdmb31pm8q3	A-APA-ISIS-041122/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			randomly generated password to use the console. The password is printed to the log, as "webAdminPass: xxx" (where "xxx") is the password. To revert to the original behaviour, the administrator would therefore need to set these configuration parameter: isis.prototyping.h2-console.web-allow-remote-access=true isis.prototyping.h2-console.generate-random-web-admin-password=false Note also that the h2 webconsole is never available in production mode, so these safeguards are only to ensure that the webconsole is secured by default also in prototype mode. **CVE ID : CVE-2022-42467**		
Affected Version(s): 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2022	6.1	Prior to 2.0.0-M9, it was possible for an end-user to set the value of an editable string property of a domain object to a value that would be rendered unchanged when the value was saved. In particular, the end-user could enter javascript or similar and this would be executed. As of this release, the	https://lists.apache.org/thread/83ftj5jgtv3mbm28w3trjyvd591jztrz	A-APA-ISIS-041122/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inputted strings are properly escaped when rendered. **CVE ID : CVE-2022-42466**		
Insecure Default Initialization of Resource	19-Oct-2022	5.3	When running in prototype mode, the h2 webconsole module (accessible from the Prototype menu) is automatically made available with the ability to directly query the database. It was felt that it is safer to require the developer to explicitly enable this capability. As of 2.0.0-M8, this can now be done using the 'isis.prototyping.h2-console.web-allow-remote-access' configuration property; the web console will be unavailable without setting this configuration. As an additional safeguard, the new 'isis.prototyping.h2-console.generate-random-web-admin-password' configuration parameter (enabled by default) requires that the administrator use a randomly generated password to use the console. The password is printed to the log, as "webAdminPass: xxx" (where "xxx") is the password. To revert to the original behaviour,	https://lists.apache.org/thread/jbv2ddt00h7ntlbm6vkk4wdmb31pm8q3	A-APA-ISIS-041122/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the administrator would therefore need to set these configuration parameter: isis.prototyping.h2-console.web-allow-remote-access=true isis.prototyping.h2-console.generate-random-web-admin-password=false Note also that the h2 webconsole is never available in production mode, so these safeguards are only to ensure that the webconsole is secured by default also in prototype mode. **CVE ID : CVE-2022-42467**		
Product: linkis					
Affected Version(s): * Up to (including) 1.2.0					
Deserialization of Untrusted Data	26-Oct-2022	8.8	In Apache Linkis <=1.2.0 when used with the MySQL Connector/J, a deserialization vulnerability with possible remote code execution impact exists when an attacker has write access to a database and configures a JDBC EC with a MySQL data source and malicious parameters. Therefore, the parameters in the jdbc url should be blacklisted. Versions of Apache Linkis <= 1.2.0 will be	https://lists.apache.org/thread/rxytj48q17304snonjtyt5lnlw64gccc	A-APA-LINK-041122/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected, We recommend users to update to 1.3.0. **CVE ID : CVE-2022-39944**		
Vendor: ARM					
Product: bifrost_gpu_kernel_driver					
Affected Version(s): From (including) r0p0 Up to (including) r38p1					
Use After Free	25-Oct-2022	8.8	An Arm product family through 2022-08-12 mail GPU kernel driver allows non-privileged users to make improper GPU processing operations to gain access to already freed memory. **CVE ID : CVE-2022-38181**	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities, https://developer.arm.com/support/arm-security-updates	A-ARM-BIFR-041122/47
Affected Version(s): r39p0					
Use After Free	25-Oct-2022	8.8	An Arm product family through 2022-08-12 mail GPU kernel driver allows non-privileged users to make improper GPU processing operations to gain access to already freed memory. **CVE ID : CVE-2022-38181**	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities, https://developer.arm.com/support/arm-security-updates	A-ARM-BIFR-041122/48
Product: midguard_gpu_kernel_driver					
Affected Version(s): From (including) r4p0 Up to (including) r31p0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	25-Oct-2022	8.8	An Arm product family through 2022-08-12 mail GPU kernel driver allows non-privileged users to make improper GPU processing operations to gain access to already freed memory. **CVE ID : CVE-2022-38181**	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities, https://developer.arm.com/support/arm-security-updates	A-ARM-MIDG-041122/49
Product: valhall_gpu_kernel_driver					
Affected Version(s): r39p0					
Use After Free	25-Oct-2022	8.8	An Arm product family through 2022-08-12 mail GPU kernel driver allows non-privileged users to make improper GPU processing operations to gain access to already freed memory. **CVE ID : CVE-2022-38181**	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities, https://developer.arm.com/support/arm-security-updates	A-ARM-VALH-041122/50
Affected Version(s): From (including) r19p0 Up to (including) r38p1					
Use After Free	25-Oct-2022	8.8	An Arm product family through 2022-08-12 mail GPU kernel driver allows non-privileged users to make improper GPU processing operations to gain access to already freed memory.	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities,	A-ARM-VALH-041122/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38181	https://developer.arm.com/support/arm-security-updates	
Vendor: Asus					
Product: asusliveupdate					
Affected Version(s): * Up to (excluding) 1.0.45.0					
N/A	18-Oct-2022	6	AsusSoftwareManager.exe in ASUS System Control Interface on ASUS personal computers (running Windows) allows a local user to write into the Temp directory and delete another more privileged file via SYSTEM privileges. This affects ASUS System Control Interface 3 before 3.1.5.0, AsusSoftwareManger.exe before 1.0.53.0, and AsusLiveUpdate.dll before 1.0.45.0. **CVE ID : CVE-2022-36439**	https://asus.com	A-ASU-ASUS-041122/52
Product: asussoftwaremanger					
Affected Version(s): * Up to (excluding) 1.0.53.0					
N/A	18-Oct-2022	6	AsusSoftwareManager.exe in ASUS System Control Interface on ASUS personal computers (running Windows) allows a local user to write into the Temp directory and delete another more privileged file via SYSTEM privileges. This affects	https://asus.com	A-ASU-ASUS-041122/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ASUS System Control Interface 3 before 3.1.5.0, AsusSoftwareManger.exe before 1.0.53.0, and AsusLiveUpdate.dll before 1.0.45.0. **CVE ID : CVE-2022-36439**		
Product: asusswitch					
Affected Version(s): * Up to (excluding) 1.0.10.0					
Incorrect Default Permissions	18-Oct-2022	7.8	AsusSwitch.exe on ASUS personal computers (running Windows) sets weak file permissions, leading to local privilege escalation (this also can be used to delete files within the system arbitrarily). This affects ASUS System Control Interface 3 before 3.1.5.0, and AsusSwitch.exe before 1.0.10.0. **CVE ID : CVE-2022-36438**	https://asus.com	A-ASU-ASUS-041122/54
Product: system_control_interface					
Affected Version(s): From (including) 3.0.0.0 Up to (excluding) 3.1.5.0					
Incorrect Default Permissions	18-Oct-2022	7.8	AsusSwitch.exe on ASUS personal computers (running Windows) sets weak file permissions, leading to local privilege escalation (this also can be used to delete files within the system arbitrarily). This affects ASUS System Control Interface 3 before 3.1.5.0, and AsusSwitch.exe before 1.0.10.0.	https://asus.com	A-ASU-SYST-041122/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36438		
N/A	18-Oct-2022	6	AsusSoftwareManager.exe in ASUS System Control Interface on ASUS personal computers (running Windows) allows a local user to write into the Temp directory and delete another more privileged file via SYSTEM privileges. This affects ASUS System Control Interface 3 before 3.1.5.0, AsusSoftwareManger.exe before 1.0.53.0, and AsusLiveUpdate.dll before 1.0.45.0. **CVE ID : CVE-2022-36439**	https://asus.com	A-ASU-SYST-041122/56
Vendor: Autodesk					
Product: autocad					
Affected Version(s): 2019					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/58
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/59
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42934**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/61
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/62
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/64
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/66
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/67
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42942**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/69
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/70
Affected Version(s): 2020					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/71

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/72
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42933		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/74
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/75
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/77
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/78
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/80
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42941		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/82
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/83
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**		
Affected Version(s): 2021					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/85
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/87
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/88
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42935**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/90
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/91
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/93
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/95
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/96
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42943**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/98
Affected Version(s): 2022					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/99
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe	https://www.autodesk.com/trust/security-	A-AUT-AUTO-041122/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/101
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42934		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/103
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/104
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/106
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/107
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe	https://www.autodesk.com/trust/security-	A-AUT-AUTO-041122/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/109
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42942		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/111
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/112
Affected Version(s): 2023					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/114
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/116
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/117
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/119
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/120
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/122
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/124
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/125
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42944**		
Product: autocad_advance_steel					
Affected Version(s): 2019					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/127
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/129
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/130
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42935**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/132
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/133
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/135
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/137
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/138
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42943**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/140
Affected Version(s): 2020					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/141
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe	https://www.autodesk.com/trust/security-	A-AUT-AUTO-041122/142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/143
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42934		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/145
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/146
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/148
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/149
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe	https://www.autodesk.com/trust/security-	A-AUT-AUTO-041122/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/151
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42942		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/153
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/154
Affected Version(s): 2021					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/156
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/158
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/159
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/161
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/162
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/164
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/166
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/167
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42944**		
Affected Version(s): 2022					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/169
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/170
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe	https://www.autodesk.com/trust/security-	A-AUT-AUTO-041122/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/172
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42935		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/174
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/175
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/177
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/178
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/180
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42943		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/182
Affected Version(s): 2023					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/183
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/185
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/187
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/188
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/190
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/191
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/193
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/195
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/196
Product: autocad_architecture					
Affected Version(s): 2019					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/198
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/200
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/201
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/203
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/204
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/206
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/208
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/209
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42944**		
Affected Version(s): 2020					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/211
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/212
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe	https://www.autodesk.com/trust/security-	A-AUT-AUTO-041122/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/214
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42935		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/216
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/217
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/219
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/220
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/222
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42943		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/224
Affected Version(s): 2021					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/225
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/227
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/229
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/230
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/232
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/233
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/235
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/237
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/238
Affected Version(s): 2022					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/240
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/241
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/243
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/245
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/246
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/248
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/249
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/251
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42944**		
Affected Version(s): 2023					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/253
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/254
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/256
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42935		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/258
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/259
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/261
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/262
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/264
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42943		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/266
Product: autocad_civil_3d					
Affected Version(s): 2019					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/267
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/269
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/271
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/272
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/274
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/275
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/277
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/279
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/280
Affected Version(s): 2020					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/282
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/283
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/285
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/287
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/288
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/290
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/291
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/293
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42944**		
Affected Version(s): 2021					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/295
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/296
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/298
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42935		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/300
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/301
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/303
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/304
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/306
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42943		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/308
Affected Version(s): 2022					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/309
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/311
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/313
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/314
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/316
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/317
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/319
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/321
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/322
Affected Version(s): 2023					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/324
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/325
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/327
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/329
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/330
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/332
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/333
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/335
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42944**		
Product: autocad_electrical					
Affected Version(s): 2019					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/337
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/338
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/340
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42935**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/342
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/343
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/345
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/346
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/348
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42943**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/350
Affected Version(s): 2020					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/351
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/353
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42934		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/355
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/356
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/358
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/359
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe	https://www.autodesk.com/trust/security-	A-AUT-AUTO-041122/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/361
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42942		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/363
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/364
Affected Version(s): 2021					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/366
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/368
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/369
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/371
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/372
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/374
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/376
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/377
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42944**		
Affected Version(s): 2022					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/379
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/380
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe	https://www.autodesk.com/trust/security-	A-AUT-AUTO-041122/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/382
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42935		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/384
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/385
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/387
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/388
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/390
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42943		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/392
Affected Version(s): 2023					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/393
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/395
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/397
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/398
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/400
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/401
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/403
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/405
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/406
Product: autocad_lt					
Affected Version(s): 2019					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/408
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/410
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/411
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/413
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/414
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/416
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/418
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/419
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42944**		
Affected Version(s): 2020					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/421
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/422
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe	https://www.autodesk.com/trust/security-	A-AUT-AUTO-041122/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/424
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42935		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/426
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/427
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/429
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/430
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/432
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42943		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/434
Affected Version(s): 2021					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/435
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/437
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/439
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/440
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/442
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/443
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/445
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/447
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/448
Affected Version(s): 2022					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/450
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/451
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/453
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/455
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/456
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/458
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/459
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/461
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42944**		
Affected Version(s): 2023					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/463
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/464
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/466
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42935		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/468
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/469
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/471
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/472
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/474
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42943		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/476
Product: autocad_map_3d					
Affected Version(s): 2019					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/477
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/479
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/481
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/482
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/484
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/485
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/487
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/489
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/490
Affected Version(s): 2020					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/492
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/493
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/495
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/497
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/498
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/500
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/501
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/503
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42944**		
Affected Version(s): 2021					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/505
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/506
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/508
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42935		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/510
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/511
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/513
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/514
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/516
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42943		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/518
Affected Version(s): 2022					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/519
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/521
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/523
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/524
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/526
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/527
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/529
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/531
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/532
Affected Version(s): 2023					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/534
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/535
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/537
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/539
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/540
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/542
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/543
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/545
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42944**		
Product: autocad_mechanical					
Affected Version(s): 2019					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/547
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/548
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/550
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42935**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/552
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/553
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/555
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/556
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/558
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42943**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/560
Affected Version(s): 2020					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/561
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/563
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42934		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/565
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/566
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/568
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/569
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe	https://www.autodesk.com/trust/security-	A-AUT-AUTO-041122/570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/571
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42942		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/573
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/574
Affected Version(s): 2021					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/576
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/578
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/579
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/581
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/582
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/584
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/586
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/587
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42944**		
Affected Version(s): 2022					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/589
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/590
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe	https://www.autodesk.com/trust/security-	A-AUT-AUTO-041122/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/592
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42935		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/594
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/595
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/597
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/598
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/600
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42943		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/602
Affected Version(s): 2023					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/603
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/605
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/607
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/608
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/610
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/611
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/613
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/615
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/616
Product: autocad_mep					
Affected Version(s): 2019					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/618
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/620
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/621
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/623
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/624
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/626
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/628
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/629
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42944**		
Affected Version(s): 2020					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/631
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/632
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe	https://www.autodesk.com/trust/security-	A-AUT-AUTO-041122/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/634
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42935		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/636
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/637
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/639
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/640
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/642
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42943		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/644
Affected Version(s): 2021					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/645
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/647
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/649
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/650
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/652
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/653
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/655
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/657
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/658
Affected Version(s): 2022					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/660
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/661
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/663
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/665
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/666
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/668
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/669
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/671
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42944**		
Affected Version(s): 2023					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/673
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/674
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/676
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42935		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/678
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/679
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/681
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/682
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/684
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42943		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/686
Product: autocad_plant_3d					
Affected Version(s): 2019					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/687
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/689
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/691
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/692
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/694
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/695
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/697
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/699
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/700
Affected Version(s): 2020					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/702
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/703
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/705
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/707
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/708
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/710
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/711
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/713
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42944**		
Affected Version(s): 2021					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/715
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/716
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/718
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42935		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/720
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/721
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/723
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/724
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to	https://www.autodesk.com/trust/security-advisories/a	A-AUT-AUTO-041122/725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/726
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42943		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/728
Affected Version(s): 2022					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/729
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/731
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/733
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/734
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to code execution in the context of the current process. **CVE ID : CVE-2022-42937**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/736
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/737
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/739
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/741
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/742
Affected Version(s): 2023					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/744
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/745
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42935**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/747
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42936**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/749
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/750
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/752
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/753
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-AUTO-041122/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42943**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/755
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-041122/756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42944**		
Product: design_review					
Affected Version(s): 2018					
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41309**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-DESI-041122/757
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41310**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-DESI-041122/758
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-DESI-041122/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42933**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42934**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-DESI-041122/760
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-DESI-041122/761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42935**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42936**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-DESI-041122/762
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42937**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-DESI-041122/763
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption	https://www.autodesk.com/trust/security-advisories/a	A-AUT-DESI-041122/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42938**	dsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42939**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-DESI-041122/765
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42940**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-DESI-041122/766
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through	https://www.autodesk.com/trust/se	A-AUT-DESI-041122/767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42941**	curity-advisories/adsk-sa-2022-0004	
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42942**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-DESI-041122/768
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-DESI-041122/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-42943**		
Out-of-bounds Write	21-Oct-2022	7.8	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42944**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-DESI-041122/770
Vendor: automox					
Product: automox					
Affected Version(s): * Up to (excluding) 40					
Incorrect Permission Assignment for Critical Resource	21-Oct-2022	7.8	The Automox Agent before 40 on Windows incorrectly sets permissions on key files. **CVE ID : CVE-2022-36122**	https://automox.com, https://www.automox.com/security/security-bulletin	A-AUT-AUTO-041122/771
Vendor: Avira					
Product: avira_security					
Affected Version(s): * Up to (including) 1.1.71.30554					
Improper Privilege Management	17-Oct-2022	8.8	A vulnerability within the Software Updater functionality of Avira Security for Windows allowed an attacker with write access to the filesystem, to escalate his	https://support.norton.com/sp/static/external/tools/security-advisories.html	A-AVI-AVIR-041122/772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges in certain scenarios. The issue was fixed with Avira Security version 1.1.72.30556. **CVE ID : CVE-2022-3368**		
Vendor: axiosys					
Product: bento4					
Affected Version(s): 1.6.0					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	5.5	Bento4 1.6.0 has memory leaks via the mp4fragment. **CVE ID : CVE-2022-40884**	N/A	A-AXI-BENT-041122/773
Affected Version(s): 1.6.0-639					
Use After Free	26-Oct-2022	7.8	A vulnerability was found in Axiomatic Bento4. It has been declared as critical. This vulnerability affects the function GetOffset of the file Ap4Sample.h of the component mp42hls. The manipulation leads to use after free. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-212002 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3662**	N/A	A-AXI-BENT-041122/774
Out-of-bounds Write	26-Oct-2022	7.8	A vulnerability classified as critical has been found in Axiomatic Bento4. Affected is the function AP4_BitStream::WriteBytes of the file	N/A	A-AXI-BENT-041122/775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ap4BitStream.cpp of the component avcinfo. The manipulation leads to heap-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-212004. **CVE ID : CVE-2022-3664**		
Out-of-bounds Write	26-Oct-2022	7.8	A vulnerability classified as critical was found in Axiomatic Bento4. Affected by this vulnerability is an unknown functionality of the file AvcInfo.cpp of the component avcinfo. The manipulation leads to heap-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-212005 was assigned to this vulnerability. **CVE ID : CVE-2022-3665**	N/A	A-AXI-BENT-041122/776
Use After Free	26-Oct-2022	7.8	A vulnerability, which was classified as critical, has been found in Axiomatic Bento4. Affected by this issue is the function AP4_LinearReader::Advance of the file Ap4LinearReader.cpp of	N/A	A-AXI-BENT-041122/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the component mp42ts. The manipulation leads to use after free. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-212006 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3666**		
Out-of-bounds Write	26-Oct-2022	7.8	A vulnerability was found in Axiomatic Bento4. It has been classified as critical. Affected is the function WriteSample of the component mp42hevc. The manipulation leads to heap-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-212010 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3670**	https://vuldb.com/?id.212010	A-AXI-BENT-041122/778
Out-of-bounds Write	26-Oct-2022	7.5	A vulnerability, which was classified as critical, was found in Axiomatic Bento4. This affects the function AP4_MemoryByteStream::WritePartial of the file Ap4ByteStream.cpp of the component mp42aac. The manipulation leads to heap-based buffer overflow. It is possible to	N/A	A-AXI-BENT-041122/779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212007. **CVE ID : CVE-2022-3667**		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	6.5	An issue was discovered in Bento4 v1.6.0-639. There is a memory leak in AP4_DescriptorFactory::CreateDescriptorFromStream in Core/Ap4DescriptorFactory.cpp, as demonstrated by mp42aac. **CVE ID : CVE-2022-43032**	N/A	A-AXI-BENT-041122/780
Use After Free	19-Oct-2022	6.5	An issue was discovered in Bento4 1.6.0-639. There is a bad free in the component AP4_HdlrAtom::~AP4_HdlrAtom() which allows attackers to cause a Denial of Service (DoS) via a crafted input. **CVE ID : CVE-2022-43033**	N/A	A-AXI-BENT-041122/781
Out-of-bounds Write	19-Oct-2022	6.5	An issue was discovered in Bento4 v1.6.0-639. There is a heap buffer overflow vulnerability in the AP4_BitReader::SkipBits(unsigned int) function in mp42ts.	N/A	A-AXI-BENT-041122/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43034		
Out-of-bounds Write	19-Oct-2022	6.5	An issue was discovered in Bento4 v1.6.0-639. There is a heap-buffer-overflow in AP4_Dec3Atom::AP4_Dec3Atom at Ap4Dec3Atom.cpp, leading to a Denial of Service (DoS), as demonstrated by mp42aac. **CVE ID : CVE-2022-43035**	N/A	A-AXI-BENT-041122/783
Missing Release of Memory after Effective Lifetime	19-Oct-2022	6.5	An issue was discovered in Bento4 1.6.0-639. There is a memory leak in the function AP4_File::ParseStream in /Core/Ap4File.cpp. **CVE ID : CVE-2022-43037**	N/A	A-AXI-BENT-041122/784
Out-of-bounds Write	19-Oct-2022	6.5	Bento4 v1.6.0-639 was discovered to contain a heap overflow via the AP4_BitReader::ReadCache() function in mp42ts. **CVE ID : CVE-2022-43038**	N/A	A-AXI-BENT-041122/785
NULL Pointer Dereference	26-Oct-2022	5.5	A vulnerability was found in Axiomatic Bento4. It has been rated as problematic. This issue affects the function AP4_StsdAtom of the file Ap4StsdAtom.cpp of the component MP4fragment. The manipulation leads to null pointer dereference. The attack may be	N/A	A-AXI-BENT-041122/786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212003. **CVE ID : CVE-2022-3663**		
Missing Release of Memory after Effective Lifetime	26-Oct-2022	5.5	A vulnerability has been found in Axiomatic Bento4 and classified as problematic. This vulnerability affects the function AP4_AtomFactory::CreateAtomFromStream of the component mp4edit. The manipulation leads to memory leak. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-212008. **CVE ID : CVE-2022-3668**	N/A	A-AXI-BENT-041122/787
Missing Release of Memory after Effective Lifetime	26-Oct-2022	5.5	A vulnerability was found in Axiomatic Bento4 and classified as problematic. This issue affects the function AP4_AvccAtom::Create of the component mp4edit. The manipulation leads to memory leak. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-	https://vuldb.com/?id.212009	A-AXI-BENT-041122/788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			212009 was assigned to this vulnerability. **CVE ID : CVE-2022-3669**		
Allocation of Resources Without Limits or Throttling	19-Oct-2022	5.5	Bento4 v1.6.0-639 has a memory allocation issue that can cause denial of service. **CVE ID : CVE-2022-40885**	N/A	A-AXI-BENT-041122/789
Vendor: Baramundi					
Product: management_suite					
Affected Version(s): 2021					
N/A	26-Oct-2022	9.8	baramundi Management Agent (bMA) in baramundi Management Suite (bMS) 2021 R1 and R2 and 2022 R1 allows remote code execution. This is fixed in 2022 R2. **CVE ID : CVE-2022-43747**	https://www.baramundi.com/de-de/security-info/s-2022-01/	A-BAR-MANA-041122/790
Affected Version(s): 2022					
N/A	26-Oct-2022	9.8	baramundi Management Agent (bMA) in baramundi Management Suite (bMS) 2021 R1 and R2 and 2022 R1 allows remote code execution. This is fixed in 2022 R2. **CVE ID : CVE-2022-43747**	https://www.baramundi.com/de-de/security-info/s-2022-01/	A-BAR-MANA-041122/791
Vendor: barangay_management_system_project					
Product: barangay_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special	28-Oct-2022	7.2	Barangay Management System v1.0 was discovered to contain a SQL injection	N/A	A-BAR-BARA-041122/792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			vulnerability via the hidden_id parameter at /clearance/clearance.php. **CVE ID : CVE-2022-43228**		
Vendor: Bestwebsoft					
Product: post_to_csv					
Affected Version(s): * Up to (including) 1.4.0					
Improper Neutralization of Formula Elements in a CSV File	25-Oct-2022	9.8	The Post to CSV by BestWebSoft WordPress plugin through 1.4.0 does not properly escape fields when exporting data as CSV, leading to a CSV injection **CVE ID : CVE-2022-3393**	https://wpscan.com/vulnerability/689b4c42-c516-4c57-8ec7-3a6f12a3594e	A-BES-POST-041122/793
Vendor: best_student_result_management_system_project					
Product: best_student_result_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Oct-2022	9.8	Best Student Result Management System v1.0 is vulnerable to SQL Injection via /upresult/upresult/notice-details.php?nid=. **CVE ID : CVE-2022-42021**	N/A	A-BES-BEST-041122/794
Vendor: billing_system_project					
Product: billing_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements	17-Oct-2022	7.2	Billing System Project v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at	N/A	A-BIL-BILL-041122/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			/phpinventory/editbrand.php. **CVE ID : CVE-2022-41498**		
Unrestricted Upload of File with Dangerous Type	18-Oct-2022	7.2	An arbitrary file upload vulnerability in the component /php_action/editProductImage.php of Billing System Project v1.0 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-41504**	N/A	A-BIL-BILL-041122/796
Vendor: bookstackapp					
Product: bookstack					
Affected Version(s): * Up to (excluding) 22.09					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Oct-2022	5.4	Cross-site scripting vulnerability in BookStack versions prior to v22.09 allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2022-40690**	https://www.bookstackapp.com/docs/admin/security/#using-bookstack-content-externally, https://www.bookstackapp.com/blog/bookstack-release-v22-09/	A-BOO-BOOK-041122/797
Vendor: boxbilling					
Product: boxbilling					
Affected Version(s): * Up to (excluding) 0.0.1					
Unrestricted Upload of File with	17-Oct-2022	7.2	Unrestricted Upload of File with Dangerous Type in GitHub repository	https://huntr.dev/bounties/c6e2973d-386d-	A-BOX-BOXB-041122/798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			boxbilling/boxbilling prior to 0.0.1. **CVE ID : CVE-2022-3552**	4667-9426-10d10828539b	
Vendor: bricksbuilder					
Product: bricks					
Affected Version(s): From (including) 1.0 Up to (including) 1.5.3					
Missing Authorization	28-Oct-2022	6.5	The Bricks theme for WordPress is vulnerable to authorization bypass due to a missing capability check on the bricks_save_post AJAX action in versions 1.0 to 1.5.3. This makes it possible for authenticated attackers with minimal permissions, such as a subscriber, to edit any page, post, or template on the vulnerable WordPress website. **CVE ID : CVE-2022-3400**	N/A	A-BRI-BRIC-041122/799
Vendor: canteen_management_system_project					
Product: canteen_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Oct-2022	9.8	A vulnerability was found in SourceCodester Canteen Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php. The manipulation of the argument business leads to sql injection. The attack can be initiated remotely. The exploit has	N/A	A-CAN-CANT-041122/800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. The identifier of this vulnerability is VDB-211192. **CVE ID : CVE-2022-3583**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Oct-2022	8.8	A vulnerability was found in SourceCodester Canteen Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file edituser.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-211193 was assigned to this vulnerability. **CVE ID : CVE-2022-3584**	N/A	A-CAN-CANT-041122/801
Unrestricted Upload of File with Dangerous Type	28-Oct-2022	7.2	Canteen Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via /youthappam/manage_website.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-43231**	N/A	A-CAN-CANT-041122/802
Improper Neutraliz	28-Oct-2022	7.2	Canteen Management System v1.0 was	N/A	A-CAN-CANT-041122/803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation of Special Elements used in an SQL Command ('SQL Injection')			discovered to contain a SQL injection vulnerability via the userid parameter at /php_action/fetchOrderData.php. **CVE ID : CVE-2022-43232**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	7.2	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the userid parameter at /php_action/fetchSelectedUser.php. **CVE ID : CVE-2022-43233**	N/A	A-CAN-CANT-041122/804
Unrestricted Upload of File with Dangerous Type	28-Oct-2022	7.2	Canteen Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via /youthappam/php_action/editProductImage.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-43275**	N/A	A-CAN-CANT-041122/805
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	7.2	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the productId parameter at /php_action/fetchSelectedfood.php. **CVE ID : CVE-2022-43276**	N/A	A-CAN-CANT-041122/806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: cashier_queuing_system_project					
Product: cashier_queuing_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Oct-2022	8.8	A vulnerability classified as critical was found in SourceCodester Cashier Queuing System 1.0. This vulnerability affects unknown code of the file /queuing/login.php of the component Login Page. The manipulation of the argument username/password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-211186 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3579**	N/A	A-CAS-CASH-041122/807
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A vulnerability, which was classified as problematic, has been found in SourceCodester Cashier Queuing System 1.0.1. This issue affects some unknown processing of the component User Creation Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-211187.	N/A	A-CAS-CASH-041122/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3580		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A vulnerability, which was classified as problematic, was found in SourceCodester Cashier Queuing System 1.0. Affected is an unknown function of the component Cashiers Tab. The manipulation of the argument Name leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-211188. **CVE ID : CVE-2022-3581**	N/A	A-CAS-CASH-041122/809
Vendor: cert					
Product: vince					
Affected Version(s): * Up to (excluding) 1.50.5					
Deserialization of Untrusted Data	26-Oct-2022	8.8	A Remote Code Injection vulnerability exists in CERT software prior to version 1.50.5. An authenticated attacker can inject arbitrary pickle object as part of a user's profile. This can lead to code execution on the server when the user's profile is accessed. **CVE ID : CVE-2022-40238**	https://github.com/CERTCC/VINCE/issues?q=label%3Asecurity	A-CER-VINC-041122/810
Vendor: Chamilo					
Product: chamilo					
Affected Version(s): 1.11.16					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	17-Oct-2022	8.8	Chamilo 1.11.16 is affected by an authenticated local file inclusion vulnerability which allows authenticated users with access to 'big file uploads' to copy/move files from anywhere in the file system into the web directory. **CVE ID : CVE-2022-42029**	https://support.chamilo.org/projects/1/wiki/Security_issues#Issue-95-2022-09-14-High-impact-Moderate-risk-Authenticated-Local-file-inclusion	A-CHA-CHAM-041122/811
Vendor: changingtec					
Product: rava_certificate_validation_system					
Affected Version(s): 3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Oct-2022	9.8	RAVA certificate validation system has insufficient validation for user input. An unauthenticated remote attacker can inject arbitrary SQL command to access, modify and delete database. **CVE ID : CVE-2022-39056**	N/A	A-CHA-RAVA-041122/812
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2022	7.5	RAVA certification validation system has a path traversal vulnerability. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and access arbitrary system files. **CVE ID : CVE-2022-39058**	N/A	A-CHA-RAVA-041122/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Oct-2022	7.2	RAVA certificate validation system has insufficient filtering for special parameter of the web page input field. A remote attacker with administrator privilege can exploit this vulnerability to perform arbitrary system command and disrupt service. **CVE ID : CVE-2022-39057**	N/A	A-CHA-RAVA-041122/814
Server-Side Request Forgery (SSRF)	18-Oct-2022	5.3	RAVA certificate validation system has inadequate filtering for URL parameter. An unauthenticated remote attacker can perform SSRF attack to discover internal network topology base on query response. **CVE ID : CVE-2022-39055**	N/A	A-CHA-RAVA-041122/815
Vendor: chop-chop					
Product: pop-up_chop_chop					
Affected Version(s): * Up to (including) 2.1.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-2022	5.4	Auth. Stored Cross-Site Scripting (XSS) in Pop-Up Chop Chop plugin <= 2.1.7 on WordPress. **CVE ID : CVE-2022-41638**	https://wordpress.org/plugins/pop-up/, https://patchstack.com/database/vulnerability/pop-up/wordpress-pop-up-chop-chop-plugin-2-1-	A-CHO-POP--041122/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				7-authenticated-stored-cross-site-scripting-xss-vulnerability?_s_id=cve	
Vendor: Cisco					
Product: identity_services_engine					
Affected Version(s): 2.7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2022	5.4	A vulnerability in the External RESTful Services (ERS) API of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by persuading an authenticated administrator of the web-based management interface to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-twLnpy3M	A-CIS-IDEN-041122/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20959		
Affected Version(s): 3.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2022	5.4	A vulnerability in the External RESTful Services (ERS) API of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by persuading an authenticated administrator of the web-based management interface to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2022-20959**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-twLnpy3M	A-CIS-IDEN-041122/818
Affected Version(s): 3.1					
Improper Input Validation	26-Oct-2022	8.1	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an	https://tools.cisco.com/security/center/content/CiscoSecurit	A-CIS-IDEN-041122/819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to read and delete files on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains certain character sequences to an affected system. A successful exploit could allow the attacker to read or delete specific files on the device that their configured administrative level should not have access to. Cisco plans to release software updates that address this vulnerability. **CVE ID : CVE-2022-20822**	yAdvisory/cisco-sa-ise-path-trav-Dz5dpzyM	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2022	5.4	A vulnerability in the External RESTful Services (ERS) API of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-twLnpy3M	A-CIS-IDEN-041122/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by persuading an authenticated administrator of the web-based management interface to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2022-20959**		
Affected Version(s): 3.2					
Improper Input Validation	26-Oct-2022	8.1	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to read and delete files on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains certain character sequences to an affected system. A successful exploit could allow the attacker to read or delete specific files on the device that their configured administrative level	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-path-trav-Dz5dpzyM	A-CIS-IDEN-041122/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should not have access to. Cisco plans to release software updates that address this vulnerability. **CVE ID : CVE-2022-20822**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2022	5.4	A vulnerability in the External RESTful Services (ERS) API of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by persuading an authenticated administrator of the web-based management interface to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2022-20959**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-twLnpy3M	A-CIS-IDEN-041122/822
Affected Version(s): From (including) 2.4 Up to (excluding) 2.7.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2022	5.4	A vulnerability in the External RESTful Services (ERS) API of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by persuading an authenticated administrator of the web-based management interface to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2022-20959**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-twLnpy3M	A-CIS-IDEN-041122/823
Product: telepresence_collaboration_endpoint					
Affected Version(s): * Up to (excluding) 10.19.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path	26-Oct-2022	7.1	Multiple vulnerabilities in Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-	A-CIS-TELE-041122/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Traversal')			data, or write arbitrary files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20955**	trav-beFvCcyu	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Oct-2022	7.1	Multiple vulnerabilities in Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive data, or write arbitrary files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20954**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-trav-beFvCcyu	A-CIS-TELE-041122/825
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Oct-2022	5.5	Multiple vulnerabilities in Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive data, or write arbitrary files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-trav-beFvCcyu	A-CIS-TELE-041122/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20953		
Affected Version(s): * Up to (excluding) 10.20.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Oct-2022	6.7	Multiple vulnerabilities in Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive data, or write arbitrary files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-trav-beFvCcyu	A-CIS-TELE-041122/827
Affected Version(s): From (including) 10.0.0.0 Up to (excluding) 10.15.2.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Oct-2022	7.2	Multiple vulnerabilities in Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive data, or write arbitrary files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20811**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-trav-beFvCcyu	A-CIS-TELE-041122/828
Affected Version(s): From (including) 9.0.0.0 Up to (excluding) 9.15.13.0					
Improper Limitatio	26-Oct-2022	7.2	Multiple vulnerabilities in Cisco TelePresence	https://tools.cisco.com/s	A-CIS-TELE-041122/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n of a Pathname to a Restricted Directory ('Path Traversal')			Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive data, or write arbitrary files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20811**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-trav-beFvCcyu	
Vendor: cleantalk					
Product: spam_protection\,_antispam\,_firewall					
Affected Version(s): * Up to (excluding) 5.185.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2022	7.2	The Spam protection, AntiSpam, FireWall by CleanTalk WordPress plugin before 5.185.1 does not validate ids before using them in a SQL statement, which could lead to SQL injection exploitable by high privilege users such as admin **CVE ID : CVE-2022-3302**	https://wpscan.com/vulnerability/1b5a018d-f2d4-4373-be1e-5162cc5c928b	A-CLE-SPAM-041122/830
Vendor: cloudflare					
Product: octorpki					
Affected Version(s): * Up to (excluding) 1.4.4					
Excessive Iteration	28-Oct-2022	7.5	Attackers can create long chains of CAs that would lead to OctoRPKI exceeding its max iterations parameter. In consequence it would cause the program to	N/A	A-CLO-OCTO-041122/831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash, preventing it from finishing the validation and leading to a denial of service. **CVE ID : CVE-2022-3616**		
Product: warp					
Affected Version(s): * Up to (excluding) 2022.8.857.0					
Missing Authorization	28-Oct-2022	9.8	It was possible to bypass policies configured for Zero Trust Secure Web Gateway by using warp-cli 'set-custom-endpoint' subcommand. Using this command with an unreachable endpoint caused the WARP Client to disconnect and allowed bypassing administrative restrictions on a Zero Trust enrolled endpoint. **CVE ID : CVE-2022-3320**	N/A	A-CLO-WARP-041122/832
Affected Version(s): * Up to (excluding) 2022.8.861.0					
Missing Authorization	28-Oct-2022	9.8	It was possible to bypass policies configured for Zero Trust Secure Web Gateway by using warp-cli 'set-custom-endpoint' subcommand. Using this command with an unreachable endpoint caused the WARP Client to disconnect and allowed bypassing administrative restrictions on a Zero Trust enrolled endpoint. **CVE ID : CVE-2022-3320**	N/A	A-CLO-WARP-041122/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2022.8.936					
Missing Authorization	28-Oct-2022	9.8	It was possible to bypass policies configured for Zero Trust Secure Web Gateway by using warp-cli 'set-custom-endpoint' subcommand. Using this command with an unreachable endpoint caused the WARP Client to disconnect and allowed bypassing administrative restrictions on a Zero Trust enrolled endpoint. **CVE ID : CVE-2022-3320**	N/A	A-CLO-WARP-041122/834
Product: warp_mobile_client					
Affected Version(s): * Up to (excluding) 6.14					
Improper Verification of Cryptographic Signature	28-Oct-2022	7.5	Lock Warp switch is a feature of Zero Trust platform which, when enabled, prevents users of enrolled devices from disabling WARP client. Due to insufficient policy verification by WARP iOS client, this feature could be bypassed by using the "Disable WARP" quick action. **CVE ID : CVE-2022-3322**	N/A	A-CLO-WARP-041122/835
Vendor: codedropz					
Product: drag_and_drop_multiple_file_upload_-_contact_form_7					
Affected Version(s): * Up to (excluding) 1.3.6.5					
Authorization Bypass Through User-	17-Oct-2022	4.3	The Drag and Drop Multiple File Upload WordPress plugin before 1.3.6.5 does not properly check for the upload size	N/A	A-COD-DRAG-041122/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Key			limit set in forms, taking the value from user input sent when submitting the form. As a result, attackers could control the file length limit and bypass the limit set by admins in the contact form. **CVE ID : CVE-2022-3282**		
Vendor: codexpert					
Product: search_logger					
Affected Version(s): * Up to (including) 0.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Oct-2022	7.2	The Search Logger WordPress plugin through 0.9 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users **CVE ID : CVE-2022-3131**	N/A	A-COD-SEAR-041122/837
Vendor: Dart					
Product: dart_software_development_kit					
Affected Version(s): * Up to (excluding) 2.18.0					
N/A	27-Oct-2022	9.8	The implementation of backslash parsing in the Dart URI class for versions prior to 2.18 and Flutter versions prior to 3.30 differs from the WhatWG URL standards. Dart uses the RFC 3986 syntax, which creates incompatibilities with the '\' characters in URIs, which can lead to auth bypass in webapps	https://github.com/dart-lang/sdk/blob/master/CHANGELOG.md#2182---2022-09-28	A-DAR-DART-041122/838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interpreting URIs. We recommend updating Dart or Flutter to mitigate the issue. **CVE ID : CVE-2022-3095**		
Vendor: dataease					
Product: dataease					
Affected Version(s): * Up to (excluding) 1.15.2					
Deserialization of Untrusted Data	25-Oct-2022	9.8	Dataease is an open source data visualization analysis tool. Dataease prior to 1.15.2 has a deserialization vulnerability. In Dataease, the Mysql data source in the data source function can customize the JDBC connection parameters and the Mysql server target to be connected. In `backend/src/main/java/io/dataease/provider/datasource/JdbcProvider.java`, the `MysqlConfiguration` class does not filter any parameters. If an attacker adds some parameters to a JDBC url and connects to a malicious mysql server, the attacker can trigger the mysql jdbc deserialization vulnerability. Through the deserialization vulnerability, the attacker can execute system commands and obtain server privileges.	https://github.com/dataease/dataease/commit/956ee2d6c9e81349a60aef435efc046888e10a6d, https://github.com/dataease/dataease/pull/3328, https://github.com/dataease/dataease/security/advisories/GHSA-q4qq-jhjv-7rh2	A-DAT-DATA-041122/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Version 1.15.2 contains a patch for this issue. **CVE ID : CVE-2022-39312**		
Vendor: datahub_project					
Product: datahub					
Affected Version(s): * Up to (excluding) 0.8.45					
Improper Verification of Cryptographic Signature	28-Oct-2022	9.8	DataHub is an open-source metadata platform. Prior to version 0.8.45, the `StatelessTokenService` of the DataHub metadata service (GMS) does not verify the signature of JWT tokens. This allows an attacker to connect to DataHub instances as any user if Metadata Service authentication is enabled. This vulnerability occurs because the `StatelessTokenService` of the Metadata service uses the `parse` method of `io.jsonwebtoken.JwtParser`, which does not perform a verification of the cryptographic token signature. This means that JWTs are accepted regardless of the used algorithm. This issue may lead to an authentication bypass. Version 0.8.45 contains a patch for the issue. There are no known workarounds.	https://github.com/datahub-project/datahub/security/advisories/GHSA-r8gm-v65f-c973	A-DAT-DATA-041122/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39366		
Vendor: Dell					
Product: emc_isilon_onefs					
Affected Version(s): * Up to (including) 8.2.2					
Incorrect Default Permissions	21-Oct-2022	4.3	The Dell Isilon OneFS versions 8.2.2 and earlier SSHD process improperly allows Transmission Control Protocol (TCP) and stream forwarding. This provides the remotesupport user and users with restricted shells more access than is intended. **CVE ID : CVE-2020-5355**	https://support.emc.com/kb/543561	A-DEL-EMC_-041122/841
Vendor: deltaww					
Product: diaenergie					
Affected Version(s): * Up to (excluding) 1.9.01.002					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Oct-2022	8.8	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a SQL injection that exists in CheckIoTHubNameExisted. A low-privileged authenticated attacker could exploit this issue to inject arbitrary SQL queries. **CVE ID : CVE-2022-40967**	N/A	A-DEL-DIAE-041122/842
Improper Neutralization of Special Elements	27-Oct-2022	8.8	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a SQL injection that exists in	N/A	A-DEL-DIAE-041122/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			GetDIAE_line_message_settingsListParameters. A low-privileged authenticated attacker could exploit this issue to inject arbitrary SQL queries. **CVE ID : CVE-2022-41133**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Oct-2022	8.8	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a SQL injection that exists in CheckDIACloud. A low-privileged authenticated attacker could exploit this issue to inject arbitrary SQL queries. **CVE ID : CVE-2022-41773**	N/A	A-DEL-DIAE-041122/844
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2022	5.4	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a stored cross-site scripting vulnerability through the PostEnergyType API. **CVE ID : CVE-2022-40965**	N/A	A-DEL-DIAE-041122/845
Improper Neutralization of Input During Web Page Generation ('Cross-site	27-Oct-2022	5.4	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a stored cross-site scripting vulnerability through the PutLineMessageSetting API. **CVE ID : CVE-2022-41555**	N/A	A-DEL-DIAE-041122/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2022	5.4	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a stored cross-site scripting vulnerability through the SetPF API. **CVE ID : CVE-2022-41651**	N/A	A-DEL-DIAE-041122/847
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2022	5.4	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a stored cross-site scripting vulnerability through the PutShift API. **CVE ID : CVE-2022-41701**	N/A	A-DEL-DIAE-041122/848
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2022	5.4	The affected product DIAEnergie (versions prior to v1.9.01.002) is vulnerable to a stored cross-site scripting vulnerability through the InsertReg API. **CVE ID : CVE-2022-41702**	N/A	A-DEL-DIAE-041122/849
Affected Version(s): 1.9.0					
Improper Neutralization of Special Elements used in an	26-Oct-2022	9.8	The HandlerPageP_KID class in Delta Electronics DIAEnergy v1.9 contains a SQL Injection flaw that could allow an attacker	N/A	A-DEL-DIAE-041122/850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			to gain code execution on a remote system. **CVE ID : CVE-2022-43774**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2022	9.8	The HICT_Loop class in Delta Electronics DIAEnergy v1.9 contains a SQL Injection flaw that could allow an attacker to gain code execution on a remote system. **CVE ID : CVE-2022-43775**	N/A	A-DEL-DIAE-041122/851
Vendor: designextreme					
Product: we\'re_open					
Affected Version(s): * Up to (excluding) 1.42					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	4.8	The Weâ€™re Open! WordPress plugin before 1.42 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-3139**	N/A	A-DES-WE\'-041122/852
Vendor: Devexpress					
Product: asp.net_web_forms_controls					
Affected Version(s): 19.2.3					
Authorization Bypass Through	18-Oct-2022	7.5	The DevExpress Resource Handler (ASPxHttpHandlerModule) in DevExpress	N/A	A-DEV-ASP.-041122/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
User-Controlled Key			ASP.NET Web Forms Build v19.2.3 does not verify the referenced objects in the /DXR.axd?r= HTTP GET parameter. This leads to an Insecure Direct Object References (IDOR) vulnerability which allows attackers to access the application source code. **CVE ID : CVE-2022-41479**		
Vendor: devhubapp					
Product: devhub					
Affected Version(s): 0.102.0					
Insufficient Session Expiration	17-Oct-2022	5.4	devhub 0.102.0 was discovered to contain a broken session control. **CVE ID : CVE-2022-41542**	https://app.devhubapp.com/, https://devhubapp.com/	A-DEV-DEVH-041122/854
Vendor: discourse					
Product: patreon					
Affected Version(s): * Up to (excluding) 2022-10-26					
Improper Authentication	26-Oct-2022	9.8	Discourse Patreon enables syncronization between Discourse Groups and Patreon rewards. On sites with Patreon login enabled, an improper authentication vulnerability could be used to take control of a victim's forum account. This vulnerability is patched in commit number 846d012151514b35ce42a1636c7d70f6dcee879e of the discourse-patreon	https://github.com/discourse/discourse-patreon/commit/846d012151514b35ce42a1636c7d70f6dcee879e, https://github.com/discourse/discourse-patreon/security/adviso	A-DIS-PATR-041122/855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plugin. Out of an abundance of caution, any Discourse accounts which have logged in with an unverified-email Patreon account will be logged out and asked to verify their email address on their next login. As a workaround, disable the patreon integration and log out all users with associated Patreon accounts. **CVE ID : CVE-2022-39355**	ries/GHSA-fvj9-f67v-qpr4	
Vendor: Djangoproject					
Product: django					
Affected Version(s): From (including) 3.2 Up to (excluding) 3.2.16					
N/A	16-Oct-2022	7.5	In Django 3.2 before 3.2.16, 4.0 before 4.0.8, and 4.1 before 4.1.2, internationalized URLs were subject to a potential denial of service attack via the locale parameter, which is treated as a regular expression. **CVE ID : CVE-2022-41323**	https://www.djangoproject.com/weblog/2022/oct/04/security-releases/,https://docs.djangoproject.com/en/4.0/releases/security/	A-DJA-DJAN-041122/856
Affected Version(s): From (including) 4.0 Up to (excluding) 4.0.8					
N/A	16-Oct-2022	7.5	In Django 3.2 before 3.2.16, 4.0 before 4.0.8, and 4.1 before 4.1.2, internationalized URLs were subject to a potential denial of service attack via the locale parameter, which	https://www.djangoproject.com/weblog/2022/oct/04/security-releases/,https://docs.djangoproject.	A-DJA-DJAN-041122/857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is treated as a regular expression. **CVE ID : CVE-2022-41323**	com/en/4.0/releases/security/	
Affected Version(s): From (including) 4.1 Up to (excluding) 4.1.2					
N/A	16-Oct-2022	7.5	In Django 3.2 before 3.2.16, 4.0 before 4.0.8, and 4.1 before 4.1.2, internationalized URLs were subject to a potential denial of service attack via the locale parameter, which is treated as a regular expression. **CVE ID : CVE-2022-41323**	https://www.djangoproject.com/weblog/2022/oct/04/security-releases/,https://docs.djangoproject.com/en/4.0/releases/security/	A-DJA-DJAN-041122/858
Vendor: dzzoffice					
Product: dzzoffice					
Affected Version(s): 2.02.1					
Cross-Site Request Forgery (CSRF)	27-Oct-2022	8.8	A Cross-Site Request Forgery (CSRF) in dzzoffice 2.02.1_SC_UTF8 allows attackers to arbitrarily create user accounts and grant Administrator rights to regular users. **CVE ID : CVE-2022-43340**	N/A	A-DZZ-DZZO-041122/859
Vendor: Eclipse					
Product: openj9					
Affected Version(s): * Up to (excluding) 0.35.0					
Access of Resource Using Incompatible Type ('Type	24-Oct-2022	6.5	In Eclipse Openj9 before version 0.35.0, interface calls can be inlined without a runtime type check. Malicious bytecode could make use	https://github.com/eclipse/omr/pull/6773, https://gitlab.eclipse.org	A-ECL-OPEN-041122/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Confusion ')			of this inlining to access or modify memory via an incompatible type. **CVE ID : CVE-2022-3676**	/eclipsefdn/emo-team/emo/-/issues/389, https://github.com/eclipse-openj9/openj9/pull/16122	
Vendor: edetw					
Product: u-office_force					
Affected Version(s): * Up to (including) 20.50.7821d					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	31-Oct-2022	6.5	U-Office Force Download function has a path traversal vulnerability. A remote attacker with general user privilege can exploit this vulnerability to download arbitrary system file. **CVE ID : CVE-2022-39023**	N/A	A-EDE-U-OF-041122/861
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	31-Oct-2022	6.5	U-Office Force Download function has a path traversal vulnerability. A remote attacker with general user privilege can exploit this vulnerability to download arbitrary system file. **CVE ID : CVE-2022-39022**	N/A	A-EDE-U-OF-041122/862
Improper Neutralization of Input During Web Page	31-Oct-2022	6.1	U-Office Force PrintMessage function has insufficient filtering for special characters. An unauthenticated remote attacker can exploit this	N/A	A-EDE-U-OF-041122/863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			vulnerability to inject JavaScript and perform XSS (Reflected Cross-Site Scripting) attack. **CVE ID : CVE-2022-39025**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Oct-2022	6.1	U-Office Force Bulletin function has insufficient filtering for special characters. An unauthenticated remote attacker can exploit this vulnerability to inject JavaScript and perform XSS (Reflected Cross-Site Scripting) attack. **CVE ID : CVE-2022-39024**	N/A	A-EDE-U-OF-041122/864
URL Redirection to Untrusted Site ('Open Redirect')	31-Oct-2022	6.1	U-Office Force login function has an Open Redirect vulnerability. An unauthenticated remote attacker can exploit this vulnerability to redirect user to arbitrary website. **CVE ID : CVE-2022-39021**	N/A	A-EDE-U-OF-041122/865
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Oct-2022	5.4	U-Office Force Forum function has insufficient filtering for special characters. A remote attacker with general user privilege can inject JavaScript and perform XSS (Stored Cross-Site Scripting) attack. **CVE ID : CVE-2022-39027**	N/A	A-EDE-U-OF-041122/866
Improper Neutraliz	31-Oct-2022	5.4	U-Office Force UserDefault page has	N/A	A-EDE-U-OF-041122/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation of Input During Web Page Generation ('Cross-site Scripting')			insufficient filtering for special characters in the HTTP header fields. A remote attacker with general user privilege can exploit this vulnerability to inject JavaScript and perform XSS (Stored Cross-Site Scripting) attack. **CVE ID : CVE-2022-39026**		
Vendor: ehoney_project					
Product: ehoney					
Affected Version(s): -					
Improper Access Control	28-Oct-2022	9.8	A vulnerability was found in seccome Ehoney. It has been rated as critical. This issue affects some unknown processing of the file /api/public/signup. The manipulation leads to improper access controls. The identifier VDB-212417 was assigned to this vulnerability. **CVE ID : CVE-2022-3735**	N/A	A-EHO-EHON-041122/868
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	9.8	A vulnerability was found in seccome Ehoney and classified as critical. Affected by this issue is some unknown functionality of the file /api/v1/bait/set. The manipulation of the argument Payload leads to sql injection. The attack may be launched remotely. VDB-212414 is	N/A	A-EHO-EHON-041122/869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3732**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	9.8	A vulnerability has been found in seccome Ehoney and classified as critical. Affected by this vulnerability is an unknown functionality of the file /api/v1/attack/token. The manipulation of the argument Payload leads to sql injection. The attack can be launched remotely. The identifier VDB-212413 was assigned to this vulnerability. **CVE ID : CVE-2022-3731**	N/A	A-EHO-EHON-041122/870
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	9.8	A vulnerability, which was classified as critical, was found in seccome Ehoney. Affected is an unknown function of the file /api/v1/attack/falco. The manipulation of the argument Payload leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-212412. **CVE ID : CVE-2022-3730**	N/A	A-EHO-EHON-041122/871
Improper Neutralization of Special	28-Oct-2022	9.8	A vulnerability, which was classified as critical, has been found in seccome Ehoney. This	N/A	A-EHO-EHON-041122/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			issue affects some unknown processing of the file /api/v1/attack. The manipulation of the argument AttackIP leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-212411. **CVE ID : CVE-2022-3729**		
Vendor: elearning_system_project					
Product: elearning_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2022	9.8	A vulnerability classified as critical was found in SourceCodester eLearning System 1.0. This vulnerability affects unknown code of the file /admin/students/manage.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-212014 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3671**	N/A	A-ELE-ELEA-041122/873
Vendor: emlog					
Product: emlog					
Affected Version(s): 1.6.0					
Unrestricted Upload of File	21-Oct-2022	7.2	Emlog Pro 1.6.0 plugins upload suffers from a	N/A	A-EML-EMLO-041122/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Dangerous Type			remote code execution (RCE) vulnerability. **CVE ID : CVE-2022-42189**		
Vendor: employee_record_management_system_project					
Product: employee_record_management_system					
Affected Version(s): 1.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	9.8	Employee Record Management System v 1.2 is vulnerable to SQL Injection via editempprofile.php. **CVE ID : CVE-2021-37782**	https://phpgurukul.com/employee-record-management-system-in-php-and-mysql/	A-EMP-EMPL-041122/875
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-2022	5.4	Employee Record Management System v 1.2 is vulnerable to Cross Site Scripting (XSS) via editempprofile.php. **CVE ID : CVE-2021-37781**	https://phpgurukul.com/employee-record-management-system-in-php-and-mysql/	A-EMP-EMPL-041122/876
Vendor: Enalean					
Product: tuleap					
Affected Version(s): From (including) 12.10 Up to (excluding) 13.12-6					
Incorrect Authorization	19-Oct-2022	5.4	Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. In versions 12.9.99.228 and above, prior to 14.0.99.24, authorizations are not properly verified when	https://tuleap.net/plugins/git/tuleap/tuleap/stable?a=commit&h=a06cb42d55c840d61a484472ed6b169ab238	A-ENA-TULE-041122/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updating the branch prefix used by the GitLab repository integration. Authenticated users can change the branch prefix of any of the GitLab repository integration they can see vie the REST endpoint `PATCH /gitlab_repositories/{id}`. This action should be restricted to Git administrators. This issue is patched in Tuleap Community Edition 14.0.99.24 and Tuleap Enterprise Edition 14.0-3. There are no known workarounds. **CVE ID : CVE-2022-39233**	53ac, https://github.com/Enalean/tuleap/security/advisories/GHSA-3884-972x-3ccq, https://tuleap.net/plugins/tracker/?aid=28848	
Affected Version(s): From (including) 12.9.99.228 Up to (excluding) 14.0.99.24					
Incorrect Authorization	19-Oct-2022	5.4	Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. In versions 12.9.99.228 and above, prior to 14.0.99.24, authorizations are not properly verified when updating the branch prefix used by the GitLab repository integration. Authenticated users can change the branch prefix of any of the GitLab repository integration they can see vie the REST endpoint `PATCH /gitlab_repositories/{id}`. This action should be restricted to Git	https://tuleap.net/plugins/git/tuleap/tuleap/stable?a=commit&h=a06cb42d55c840d61a484472ed6b169ab23853ac, https://github.com/Enalean/tuleap/security/advisories/GHSA-3884-972x-3ccq, https://tuleap.net/plugins/tracker/?aid=28848	A-ENA-TULE-041122/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrators. This issue is patched in Tuleap Community Edition 14.0.99.24 and Tuleap Enterprise Edition 14.0-3. There are no known workarounds. **CVE ID : CVE-2022-39233**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14.0-3					
Incorrect Authorization	19-Oct-2022	5.4	Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. In versions 12.9.99.228 and above, prior to 14.0.99.24, authorizations are not properly verified when updating the branch prefix used by the GitLab repository integration. Authenticated users can change the branch prefix of any of the GitLab repository integration they can see vie the REST endpoint `PATCH /gitlab_repositories/{id}`. This action should be restricted to Git administrators. This issue is patched in Tuleap Community Edition 14.0.99.24 and Tuleap Enterprise Edition 14.0-3. There are no known workarounds. **CVE ID : CVE-2022-39233**	https://tuleap.net/plugins/git/tuleap/tuleap/stable?a=commit&h=a06cb42d55c840d61a484472ed6b169ab23853ac, https://github.com/Enalean/tuleap/security/advisories/GHSA-3884-972x-3ccq, https://tuleap.net/plugins/tracker/?aid=28848	A-ENA-TULE-041122/879
Vendor: Esri					
Product: arcgis_server					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 10.9.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Oct-2022	8.1	Esri ArcGIS Server versions 10.9.1 and prior have a path traversal vulnerability that may result in a denial of service by allowing a remote, authenticated attacker to overwrite internal ArcGIS Server directory. **CVE ID : CVE-2022-38196**	https://www.esri.com/arcgis-blog/products/administration/administration/arcgis-server-security-2022-update-1-patch	A-ESR-ARCG-041122/880
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2022	6.1	There is as reflected cross site scripting issue in Esri ArcGIS Server versions 10.9.1 and below which may allow a remote unauthorized attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the victim's browser. **CVE ID : CVE-2022-38195**	https://www.esri.com/arcgis-blog/products/administration/administration/arcgis-server-security-2022-update-1-patch	A-ESR-ARCG-041122/881
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2022	6.1	There is a reflected cross site scripting issue in the Esri ArcGIS Server services directory versions 10.9.1 and below that may allow a remote, unauthenticated attacker to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the victim's browser. **CVE ID : CVE-2022-38198**	https://www.esri.com/arcgis-blog/products/administration/administration/arcgis-server-security-2022-update-1-patch	A-ESR-ARCG-041122/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	25-Oct-2022	6.1	Esri ArcGIS Server versions 10.9.1 and below have an unvalidated redirect issue that may allow a remote, unauthenticated attacker to phish a user into accessing an attacker controlled website via a crafted query parameter. **CVE ID : CVE-2022-38197**	https://www.esri.com/arcgis-blog/products/administration/administration/arcgis-server-security-2022-update-1-patch	A-ESR-ARCG-041122/883
Affected Version(s): 10.7.1					
Download of Code Without Integrity Check	25-Oct-2022	6.1	A remote file download issue can occur in some capabilities of Esri ArcGIS Server web services that may in some edge cases allow a remote, unauthenticated attacker to induce an unsuspecting victim to launch a process in the victim's PATH environment. Current browsers provide users with warnings against running unsigned executables downloaded from the internet. **CVE ID : CVE-2022-38199**	https://www.esri.com/arcgis-blog/products/administration/administration/arcgis-server-security-2022-update-1-patch	A-ESR-ARCG-041122/884
Improper Neutralization of Input During Web Page Generation ('Cross-site	25-Oct-2022	6.1	A cross site scripting vulnerability exists in some map service configurations of ArcGIS Server versions 10.8.1 and 10.7.1. Specifically crafted web requests can execute arbitrary	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-server-map-	A-ESR-ARCG-041122/885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			JavaScript in the context of the victim's browser. **CVE ID : CVE-2022-38200**	service-security-2022-update-1-is-now-available	
Affected Version(s): 10.8.1					
Download of Code Without Integrity Check	25-Oct-2022	6.1	A remote file download issue can occur in some capabilities of Esri ArcGIS Server web services that may in some edge cases allow a remote, unauthenticated attacker to induce an unsuspecting victim to launch a process in the victim's PATH environment. Current browsers provide users with warnings against running unsigned executables downloaded from the internet. **CVE ID : CVE-2022-38199**	https://www.esri.com/arcgis-blog/products/administration/administration/arcgis-server-security-2022-update-1-patch	A-ESR-ARCG-041122/886
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2022	6.1	A cross site scripting vulnerability exists in some map service configurations of ArcGIS Server versions 10.8.1 and 10.7.1. Specifically crafted web requests can execute arbitrary JavaScript in the context of the victim's browser. **CVE ID : CVE-2022-38200**	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-server-map-service-security-2022-update-1-is-now-available	A-ESR-ARCG-041122/887
Affected Version(s): 10.9.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Download of Code Without Integrity Check	25-Oct-2022	6.1	A remote file download issue can occur in some capabilities of Esri ArcGIS Server web services that may in some edge cases allow a remote, unauthenticated attacker to induce an unsuspecting victim to launch a process in the victim's PATH environment. Current browsers provide users with warnings against running unsigned executables downloaded from the internet. **CVE ID : CVE-2022-38199**	https://www.esri.com/arcgis-blog/products/administration/administration/arcgis-server-security-2022-update-1-patch	A-ESR-ARCG-041122/888
Vendor: eve-ng					
Product: eve-ng					
Affected Version(s): 2.0.3-112					
Unrestricted Upload of File with Dangerous Type	20-Oct-2022	7.2	An arbitrary file upload vulnerability in the apiImportLabs function in api_labs.php of EVE-NG 2.0.3-112 Community allows attackers to execute arbitrary code via a crafted UNL file. **CVE ID : CVE-2022-31366**	http://eve-ng.com	A-EVE-EVE--041122/889
Vendor: evm_project					
Product: evm					
Affected Version(s): * Up to (excluding) 0.36.0					
Always-Incorrect Control Flow	25-Oct-2022	7.5	SputnikVM, also called evm, is a Rust implementation of Ethereum Virtual Machine. A custom stateful precompile can	https://github.com/rust-blockchain/evm/pull/133,	A-EVM-EVM-041122/890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Implementation			use the `is_static` parameter to determine if the call is executed in a static context (via `STATICCALL`), and thus decide if stateful operations should be done. Prior to version 0.36.0, the passed `is_static` parameter was incorrect -- it was only set to `true` if the call came from a direct `STATICCALL` opcode. However, once a static call context is entered, it should stay static. The issue only impacts custom precompiles that actually uses `is_static`. For those affected, the issue can lead to possible incorrect state transitions. Version 0.36.0 contains a patch. There are no known workarounds. **CVE ID : CVE-2022-39354**	https://github.com/rust-blockchain/evm/security/advisories/GHSA-hhc4-47rh-cr34	
Vendor: Exim					
Product: exim					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Oct-2022	7.5	A vulnerability was found in Exim and classified as problematic. This issue affects some unknown processing of the component Regex Handler. The manipulation leads to use after free. The name of the patch is	https://git.exim.org/exim.git/commit/4e9ed49f8f12eb331b29bd5b6dc3693c520fddc2, https://bugs.exim.org/sh	A-EXI-EXIM-041122/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4e9ed49f8f12eb331b29bd5b6dc3693c520fddc2. It is recommended to apply a patch to fix this issue. The identifier VDB-211073 was assigned to this vulnerability. **CVE ID : CVE-2022-3559**	ow_bug.cgi?id=2915	
Affected Version(s): 2022-10-18					
Use After Free	20-Oct-2022	9.8	A vulnerability was found in Exim and classified as problematic. This issue affects the function dmarc_dns_lookup of the file dmarc.c of the component DMARC Handler. The manipulation leads to use after free. The attack may be initiated remotely. The name of the patch is 12fb3842f81bcbd4a4519d5728f2d7e0e3ca1445. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211919. **CVE ID : CVE-2022-3620**	https://git.exim.org/exim.git/commit/12fb3842f81bcbd4a4519d5728f2d7e0e3ca1445	A-EXI-EXIM-041122/892
Vendor: Exiv2					
Product: exiv2					
Affected Version(s): * Up to (excluding) 2022-09-29					
Out-of-bounds Write	27-Oct-2022	9.8	A vulnerability has been found in Exiv2 and classified as critical. This vulnerability affects the	https://github.com/Exiv2/exiv2/commit/a38e1	A-EXI-EXIV-041122/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function QuickTimeVideo::userDataDecoder of the file quicktimevideo.cpp of the component QuickTime Video Handler. The manipulation leads to heap-based buffer overflow. The attack can be initiated remotely. The name of the patch is a38e124076138e529774d5ec9890d0731058115a. It is recommended to apply a patch to fix this issue. VDB-212350 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3719**	24076138e529774d5ec9890d0731058115a	
Affected Version(s): * Up to (excluding) 2022-10-08					
NULL Pointer Dereference	27-Oct-2022	6.5	A vulnerability, which was classified as problematic, was found in Exiv2. This affects the function QuickTimeVideo::decodeBlock of the file quicktimevideo.cpp of the component QuickTime Video Handler. The manipulation leads to null pointer dereference. It is possible to initiate the attack remotely. The name of the patch is 459910c36a21369c09b75bcfa82f287c9da56abf. It is recommended to apply a patch to fix this issue. The identifier VDB-	https://github.com/Exiv2/exiv2/commit/459910c36a21369c09b75bcfa82f287c9da56abf	A-EXI-EXIV-041122/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			212349 was assigned to this vulnerability. **CVE ID : CVE-2022-3718**		
Affected Version(s): * Up to (excluding) 2022-10-24					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Oct-2022	9.8	A vulnerability, which was classified as critical, has been found in Exiv2. Affected by this issue is the function BmffImage::boxHandler of the file bmffimage.cpp. The manipulation leads to memory corruption. The attack may be launched remotely. The name of the patch is a58e52ed702d3bc7b8bab7ec1d70a4849eebece3. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-212348. **CVE ID : CVE-2022-3717**	https://github.com/Exiv2/exiv2/commit/a58e52ed702d3bc7b8bab7ec1d70a4849eebece3	A-EXI-EXIV-041122/895
Vendor: expresstech					
Product: quiz_and_survey_master					
Affected Version(s): * Up to (including) 7.3.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	7.2	Auth. SQL Injection (SQLi) vulnerability in Quiz And Survey Master plugin <= 7.3.4 on WordPress. **CVE ID : CVE-2021-36898**	https://patchstack.com/database/vulnerability/quiz-master-next/wordpress-quiz-and-survey-master-plugin-7-3-4-auth-sql-injection-	A-EXP-QUIZ-041122/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				sqli-vulnerability?_s_id=cve, https://wordpress.org/plugins/quiz-master-next/#developers	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-2022	5.4	Auth. (editor+) Reflected Cross-Site Scripting (XSS) vulnerability in ExpressTech Quiz And Survey Master plugin <= 7.3.4 on WordPress. **CVE ID : CVE-2021-36864**	https://patchstack.com/database/vulnerability/quiz-master-next/wordpress-quiz-and-survey-master-plugin-7-3-4-auth-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve, https://wordpress.org/plugins/quiz-master-next/#developers	A-EXP-QUIZ-041122/897
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-2022	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in ExpressTech Quiz And Survey Master plugin <= 7.3.4 on WordPress. **CVE ID : CVE-2021-36863**	https://wordpress.org/plugins/quiz-master-next/#developers, https://patchstack.com/database/vulnerability/quiz-master-	A-EXP-QUIZ-041122/898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				next/wordpress-quiz-and-survey-master-plugin-7-3-4-auth-stored-cross-site-scripting-xss-vulnerability?_s_id=cve	
Vendor: extended_keccak_code_package_project					
Product: extended_keccak_code_package					
Affected Version(s): -					
Integer Overflow or Wraparound	21-Oct-2022	9.8	The Keccak XKCP SHA-3 reference implementation before fdc6fef has an integer overflow and resultant buffer overflow that allows attackers to execute arbitrary code or eliminate expected cryptographic properties. This occurs in the sponge function interface. **CVE ID : CVE-2022-37454**	https://github.com/XKCP/XKCP/security/advisories/GHSA-6w4m-2xhg-2658	A-EXT-EXTE-041122/899
Vendor: eyoucms					
Product: eyoucms					
Affected Version(s): 1.5.9					
Cross-Site Request Forgery (CSRF)	18-Oct-2022	8.8	EyouCMS V1.5.9 was discovered to contain multiple Cross-Site Request Forgery (CSRF) vulnerabilities via the Members Center, Editorial Membership,	N/A	A-EYO-EYOU-041122/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Points Recharge components. **CVE ID : CVE-2022-41500**		
Vendor: F5					
Product: big-ip_access_policy_manager					
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.5.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/901
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/902
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Uncontrolled Resource	19-Oct-2022	7.5	In all BIG-IP 13.1.x versions, when an iRule containing the HTTP::collect command is configured on a virtual	https://support.f5.com/csp/article/K69940053	A-F5-BIG--041122/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			server, undisclosed requests can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41833**		
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/904
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/905
Cleartext Transmission of Sensitive	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/907
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections.	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36795		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/909
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/910
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/912
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/913
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/915
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/917
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/918
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/920
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/921
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**		
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/923
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/925
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/926
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization.	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41832		
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/928
Product: big-ip_advanced_firewall_manager					
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.5.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/929
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Uncontrolled Resource Consumption	19-Oct-2022	7.5	In all BIG-IP 13.1.x versions, when an iRule containing the HTTP::collect command is configured on a virtual server, undisclosed requests can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41833**	https://support.f5.com/csp/article/K69940053	A-F5-BIG--041122/931
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/932
Improper Input Validation	19-Oct-2022	6.5	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when BIG-IP is provisioned with PEM or AFM module, an undisclosed input can cause Traffic	https://support.f5.com/csp/article/K93723284	A-F5-BIG--041122/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41813**		
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/934
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/935
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Input Validation	19-Oct-2022	6.5	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of	https://support.f5.com/c	A-F5-BIG--041122/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13.1.x, when BIG-IP is provisioned with PEM or AFM module, an undisclosed input can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41813**	sp/article/K93723284	
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/937
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/939
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/940
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/942
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/943
Improper Input Validation	19-Oct-2022	6.5	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when BIG-IP is provisioned with PEM or AFM module, an	https://support.f5.com/csp/article/K93723284	A-F5-BIG--041122/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed input can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41813**		
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/945
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/946
Missing Release of Memory after	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x	https://support.f5.com/c	A-F5-BIG--041122/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	sp/article/K43024307	
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/948
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/950
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/951
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increase in memory resource utilization. **CVE ID : CVE-2022-41832**		
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/953
Improper Input Validation	19-Oct-2022	6.5	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when BIG-IP is provisioned with PEM or AFM module, an undisclosed input can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41813**	https://support.f5.com/csp/article/K93723284	A-F5-BIG--041122/954
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/956
Uncontrolled Resource Consumption	19-Oct-2022	7.5	In versions 16.1.x before 16.1.3.2 and 15.1.x before 15.1.5.1, when BIG-IP AFM Network Address Translation policy with IPv6/IPv4 translation rules is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41806**	https://support.f5.com/csp/article/K00721320	A-F5-BIG--041122/957
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x	https://support.f5.com/c	A-F5-BIG--041122/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	sp/article/K52494562	
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/959
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/960
Uncontrolled	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x	https://support.f5.com/c	A-F5-BIG--041122/961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	sp/article/K22505850	
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.5.1					
Uncontrolled Resource Consumption	19-Oct-2022	7.5	In versions 16.1.x before 16.1.3.2 and 15.1.x before 15.1.5.1, when BIG-IP AFM Network Address Translation policy with IPv6/IPv4 translation rules is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41806**	https://support.f5.com/csp/article/K00721320	A-F5-BIG--041122/962
Product: big-ip_advanced_web_application_firewall					
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.5.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Oct-2022	7.2	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, When the Advanced WAF / ASM module is provisioned, an authenticated remote code execution vulnerability exists in the	https://support.f5.com/csp/article/K11830089	A-F5-BIG--041122/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIG-IP iControl REST interface. **CVE ID : CVE-2022-41617**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/964
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Oct-2022	7.2	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, When the Advanced WAF / ASM module is provisioned, an authenticated remote code execution vulnerability exists in the BIG-IP iControl REST interface. **CVE ID : CVE-2022-41617**	https://support.f5.com/csp/article/K11830089	A-F5-BIG--041122/965
Cleartext Transmission of	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before	https://support.f5.com/c	A-F5-BIG--041122/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	sp/article/K31523465	
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.2					
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	When a BIG-IP Advanced WAF/ASM security policy is configured on a virtual server, undisclosed requests can cause the bd process to terminate. **CVE ID : CVE-2022-41691**	https://support.f5.com/csp/article/K02694732	A-F5-BIG--041122/967
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Oct-2022	7.2	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, When the Advanced WAF / ASM module is provisioned, an authenticated remote code execution vulnerability exists in the BIG-IP iControl REST interface. **CVE ID : CVE-2022-41617**	https://support.f5.com/csp/article/K11830089	A-F5-BIG--041122/968
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Oct-2022	7.5	When an 'Attack Signature False Positive Mode' enabled security policy is configured on a virtual server, undisclosed requests can cause the bd process to terminate. **CVE ID : CVE-2022-41836**	https://support.f5.com/csp/article/K47204506	A-F5-BIG--041122/969
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/970
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
N/A	19-Oct-2022	7.5	When an 'Attack Signature False Positive Mode' enabled security policy is configured on a virtual server, undisclosed requests can cause the bd process to terminate. **CVE ID : CVE-2022-41836**	https://support.f5.com/csp/article/K47204506	A-F5-BIG--041122/971
Improper Neutralization of Special	19-Oct-2022	7.2	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x	https://support.f5.com/c	A-F5-BIG--041122/972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			before 13.1.5.1, When the Advanced WAF / ASM module is provisioned, an authenticated remote code execution vulnerability exists in the BIG-IP iControl REST interface. **CVE ID : CVE-2022-41617**	sp/article/K11830089	
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/973
Affected Version(s): 17.0.0					
N/A	19-Oct-2022	7.5	When an 'Attack Signature False Positive Mode' enabled security policy is configured on a virtual server, undisclosed requests can cause the bd process to terminate. **CVE ID : CVE-2022-41836**	https://support.f5.com/csp/article/K47204506	A-F5-BIG--041122/974
Product: big-ip_analytics					
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.5.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/975
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/976
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Uncontrolled Resource Consumption	19-Oct-2022	7.5	In all BIG-IP 13.1.x versions, when an iRule containing the HTTP::collect command is configured on a virtual server, undisclosed requests can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41833**	https://support.f5.com/csp/article/K69940053	A-F5-BIG--041122/977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/978
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/979
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/981
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/982
Missing Release of Memory after	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**		
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/984
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/985
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/986
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/987
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate.	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41694		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/989
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/990
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**		
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/992
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/993
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/994
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/995
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests.	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41770		
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/997
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/998
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1000
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1001
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**		
Product: big-ip_application_acceleration_manager					
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.5.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1003
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1004
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	19-Oct-2022	7.5	In all BIG-IP 13.1.x versions, when an iRule containing the HTTP::collect command is configured on a virtual server, undisclosed requests can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41833**	https://support.f5.com/csp/article/K69940053	A-F5-BIG--041122/1005
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1006
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1008
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1009
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1011
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1012
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1014
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1016
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1017
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increase in memory resource utilization. **CVE ID : CVE-2022-41624**		
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1019
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1020
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1022
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1024
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1025
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1027
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1028
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**		
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1030
Product: big-ip_application_security_manager					
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.5.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1031
Missing Release of Memory	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x	https://support.f5.com/c	A-F5-BIG--041122/1032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
after Effective Lifetime			before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	sp/article/K10347453	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Oct-2022	7.2	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, When the Advanced WAF / ASM module is provisioned, an authenticated remote code execution vulnerability exists in the BIG-IP iControl REST interface. **CVE ID : CVE-2022-41617**	https://support.f5.com/csp/article/K11830089	A-F5-BIG--041122/1033
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Uncontrolled Resource Consumption	19-Oct-2022	7.5	In all BIG-IP 13.1.x versions, when an iRule containing the HTTP::collect command is configured on a virtual server, undisclosed requests can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41833**	https://support.f5.com/csp/article/K69940053	A-F5-BIG--041122/1034
Uncontrolled Resource	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x	https://support.f5.com/c	A-F5-BIG--041122/1035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	sp/article/K22505850	
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1036
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause MCPD to terminate. **CVE ID : CVE-2022-41694**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1038
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1039
Improper Neutralization of Special Elements used in a Command ('Comma	19-Oct-2022	7.2	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, When the Advanced WAF / ASM module is provisioned, an	https://support.f5.com/csp/article/K11830089	A-F5-BIG--041122/1040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
nd Injection')			authenticated remote code execution vulnerability exists in the BIG-IP iControl REST interface. **CVE ID : CVE-2022-41617**		
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1041
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1042
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1043
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	When a BIG-IP Advanced WAF/ASM security policy is configured on a virtual server, undisclosed requests can cause the bd process to terminate. **CVE ID : CVE-2022-41691**	https://support.f5.com/csp/article/K02694732	A-F5-BIG--041122/1044
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1045
Improper Neutralization of Special	19-Oct-2022	7.2	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x	https://support.f5.com/c	A-F5-BIG--041122/1046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			before 13.1.5.1, When the Advanced WAF / ASM module is provisioned, an authenticated remote code execution vulnerability exists in the BIG-IP iControl REST interface. **CVE ID : CVE-2022-41617**	sp/article/K11830089	
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1047
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1049
N/A	19-Oct-2022	7.5	When an 'Attack Signature False Positive Mode' enabled security policy is configured on a virtual server, undisclosed requests can cause the bd process to terminate. **CVE ID : CVE-2022-41836**	https://support.f5.com/csp/article/K47204506	A-F5-BIG--041122/1050
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1051
Cleartext Transmission of	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before	https://support.f5.com/c	A-F5-BIG--041122/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	sp/article/K31523465	
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1053
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to stop processing new client connections. **CVE ID : CVE-2022-36795**		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1055
N/A	19-Oct-2022	7.5	When an 'Attack Signature False Positive Mode' enabled security policy is configured on a virtual server, undisclosed requests can cause the bd process to terminate. **CVE ID : CVE-2022-41836**	https://support.f5.com/csp/article/K47204506	A-F5-BIG--041122/1056
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Oct-2022	7.2	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, When the Advanced WAF / ASM module is provisioned, an authenticated remote code execution vulnerability exists in the BIG-IP iControl REST interface.	https://support.f5.com/csp/article/K11830089	A-F5-BIG--041122/1057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41617		
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1058
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1059
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1061
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1062
Affected Version(s): 17.0.0					
N/A	19-Oct-2022	7.5	When an 'Attack Signature False Positive Mode' enabled security	https://support.f5.com/c	A-F5-BIG--041122/1063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			policy is configured on a virtual server, undisclosed requests can cause the bd process to terminate. **CVE ID : CVE-2022-41836**	sp/article/K47204506	
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.5					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1064
Affected Version(s): From (including) 17.0.0 Up to (including) 17.0.0.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1065
Missing Release of	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x	https://support.f5.com/c	A-F5-BIG--041122/1066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	sp/article/K43024307	
Product: big-ip_application_visibility_and_reporting					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1067
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1069
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied.	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41983		
Product: big-ip_carrier-grade_nat					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1071
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1072
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1073
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1074
Product: big-ip_ddos_hybrid_defender					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cleartext Transmission of Sensitive	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1076
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1078
Product: big-ip_domain_name_system					
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.5.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when DNS profile is configured on a virtual server with DNS Express enabled, undisclosed DNS queries with DNSSEC can cause TMM to terminate. **CVE ID : CVE-2022-41787**	https://support.f5.com/csp/article/K70569537	A-F5-BIG--041122/1080
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1081
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Uncontrolled Resource Consumption	19-Oct-2022	7.5	In all BIG-IP 13.1.x versions, when an iRule containing the HTTP::collect command is configured on a virtual server, undisclosed requests can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41833**	https://support.f5.com/csp/article/K69940053	A-F5-BIG--041122/1082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1083
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1084
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1086
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1087
NULL Pointer Dereference	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and	https://support.f5.com/csp/article/K70569537	A-F5-BIG--041122/1088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13.1.x before 13.1.5.1, when DNS profile is configured on a virtual server with DNS Express enabled, undisclosed DNS queries with DNSSEC can cause TMM to terminate. **CVE ID : CVE-2022-41787**		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1089
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1090
Cleartext Transmission of	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before	https://support.f5.com/c	A-F5-BIG--041122/1091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	sp/article/K31523465	
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1092
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
NULL Pointer Dereference	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when DNS profile is configured on a virtual server with DNS Express enabled, undisclosed DNS queries with	https://support.f5.com/csp/article/K70569537	A-F5-BIG--041122/1093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNSSEC can cause TMM to terminate. **CVE ID : CVE-2022-41787**		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1094
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1095
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1097
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1098
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1100
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections.	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36795		
NULL Pointer Dereference	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when DNS profile is configured on a virtual server with DNS Express enabled, undisclosed DNS queries with DNSSEC can cause TMM to terminate. **CVE ID : CVE-2022-41787**	https://support.f5.com/csp/article/K70569537	A-F5-BIG--041122/1102
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1103
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**		
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1105
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1106
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1108
NULL Pointer Dereference	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when DNS profile is configured on a virtual server with DNS Express enabled, undisclosed DNS queries with DNSSEC can cause TMM to terminate. **CVE ID : CVE-2022-41787**	https://support.f5.com/csp/article/K70569537	A-F5-BIG--041122/1109
Missing Release of	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x	https://support.f5.com/c	A-F5-BIG--041122/1110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	sp/article/K10347453	
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1111
Product: big-ip_edge_gateway					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1113
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1114
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1115
Product: big-ip_fraud_protection_service					
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.5.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1116
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Uncontrolled Resource Consumption	19-Oct-2022	7.5	In all BIG-IP 13.1.x versions, when an iRule containing the HTTP::collect command is configured on a virtual server, undisclosed requests can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41833**	https://support.f5.com/csp/article/K69940053	A-F5-BIG--041122/1118
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1119
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**		
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1121
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1122
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1123
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1124
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests.	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41770		
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1126
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1127
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**		
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1129
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1130
Missing Release of Memory after	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x	https://support.f5.com/c	A-F5-BIG--041122/1131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	sp/article/K43024307	
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1132
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1134
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1135
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**		
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1137
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1138
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1140
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1141
Uncontrolled Resource	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x	https://support.f5.com/c	A-F5-BIG--041122/1142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	sp/article/K22505850	
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1143
Product: big-ip_global_traffic_manager					
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.5.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increase in memory resource utilization. **CVE ID : CVE-2022-41624**		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1145
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Uncontrolled Resource Consumption	19-Oct-2022	7.5	In all BIG-IP 13.1.x versions, when an iRule containing the HTTP::collect command is configured on a virtual server, undisclosed requests can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41833**	https://support.f5.com/csp/article/K69940053	A-F5-BIG--041122/1146
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**		
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1148
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1149
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1151
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1153
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1154
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1156
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1157
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1159
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1160
Cleartext Transmission of	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before	https://support.f5.com/c	A-F5-BIG--041122/1161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	sp/article/K31523465	
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1162
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to stop processing new client connections. **CVE ID : CVE-2022-36795**		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1164
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1165
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1167
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1168
Missing Release of	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x	https://support.f5.com/c	A-F5-BIG--041122/1169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	sp/article/K43024307	
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1170
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1171
Product: big-ip_link_controller					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.5.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1172
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1173
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Uncontrolled Resource Consumption	19-Oct-2022	7.5	In all BIG-IP 13.1.x versions, when an iRule containing the HTTP::collect command is configured on a virtual server, undisclosed requests can cause Traffic Management Microkernel (TMM) to terminate.	https://support.f5.com/csp/article/K69940053	A-F5-BIG--041122/1174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41833		
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1175
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1176
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1178
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1179
Missing Release of	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x	https://support.f5.com/c	A-F5-BIG--041122/1180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	sp/article/K10347453	
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1181
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied.	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41983		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1183
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1184
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system,	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1186
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1187
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**		
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1189
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1191
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1192
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**		
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1194
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1195
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1197
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1198
Uncontrolled Resource	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x	https://support.f5.com/c	A-F5-BIG--041122/1199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	sp/article/K22505850	
Product: big-ip_local_traffic_manager					
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.5.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1200
NULL Pointer Dereference	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when DNS profile is configured on a virtual server with DNS Express enabled, undisclosed DNS queries with DNSSEC can cause TMM to terminate.	https://support.f5.com/csp/article/K70569537	A-F5-BIG--041122/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41787		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1202
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Uncontrolled Resource Consumption	19-Oct-2022	7.5	In all BIG-IP 13.1.x versions, when an iRule containing the HTTP::collect command is configured on a virtual server, undisclosed requests can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41833**	https://support.f5.com/csp/article/K69940053	A-F5-BIG--041122/1203
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests.	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41770		
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1205
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1206
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1208
NULL Pointer Dereference	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when DNS profile is configured on a virtual server with DNS Express enabled, undisclosed DNS queries with DNSSEC can cause TMM to terminate. **CVE ID : CVE-2022-41787**	https://support.f5.com/csp/article/K70569537	A-F5-BIG--041122/1209
Missing Release of Memory	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x	https://support.f5.com/c	A-F5-BIG--041122/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
after Effective Lifetime			before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	sp/article/K10347453	
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1211
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied.	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41983		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1213
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
NULL Pointer Dereference	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when DNS profile is configured on a virtual server with DNS Express enabled, undisclosed DNS queries with DNSSEC can cause TMM to terminate. **CVE ID : CVE-2022-41787**	https://support.f5.com/csp/article/K70569537	A-F5-BIG--041122/1214
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**		
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1216
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1217
Missing Release of Memory after	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1,	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**		
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1219
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1220
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1221
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1222
NULL Pointer Dereference	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when DNS profile is configured on a virtual server with DNS Express enabled, undisclosed DNS queries with	https://support.f5.com/csp/article/K70569537	A-F5-BIG--041122/1223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNSSEC can cause TMM to terminate. **CVE ID : CVE-2022-41787**		
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1224
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1225
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1227
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1228
Missing Release of	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x	https://support.f5.com/c	A-F5-BIG--041122/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	sp/article/K43024307	
NULL Pointer Dereference	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when DNS profile is configured on a virtual server with DNS Express enabled, undisclosed DNS queries with DNSSEC can cause TMM to terminate. **CVE ID : CVE-2022-41787**	https://support.f5.com/csp/article/K70569537	A-F5-BIG--041122/1230
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1232
Product: big-ip_policy_enforcement_manager					
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.5.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1233
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increase in memory resource utilization. **CVE ID : CVE-2022-41832**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Uncontrolled Resource Consumption	19-Oct-2022	7.5	In all BIG-IP 13.1.x versions, when an iRule containing the HTTP::collect command is configured on a virtual server, undisclosed requests can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41833**	https://support.f5.com/csp/article/K69940053	A-F5-BIG--041122/1235
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1236
Improper Input Validation	19-Oct-2022	6.5	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when BIG-IP is provisioned with PEM or AFM module, an undisclosed input can cause Traffic Management	https://support.f5.com/csp/article/K93723284	A-F5-BIG--041122/1237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41813**		
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1238
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1239
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Input Validation	19-Oct-2022	6.5	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when BIG-IP is	https://support.f5.com/csp/article/K93723284	A-F5-BIG--041122/1240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provisioned with PEM or AFM module, an undisclosed input can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41813**		
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1241
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1243
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1244
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1246
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1247
Improper Input Validation	19-Oct-2022	6.5	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when BIG-IP is provisioned with PEM or AFM module, an	https://support.f5.com/csp/article/K93723284	A-F5-BIG--041122/1248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed input can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41813**		
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1249
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1250
Missing Release of Memory after	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x	https://support.f5.com/c	A-F5-BIG--041122/1251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	sp/article/K43024307	
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1252
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Input Validation	19-Oct-2022	4.9	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate. **CVE ID : CVE-2022-41694**	https://support.f5.com/csp/article/K64829234	A-F5-BIG--041122/1254
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1255
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increase in memory resource utilization. **CVE ID : CVE-2022-41832**		
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1257
Improper Input Validation	19-Oct-2022	6.5	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when BIG-IP is provisioned with PEM or AFM module, an undisclosed input can cause Traffic Management Microkernel (TMM) to terminate. **CVE ID : CVE-2022-41813**	https://support.f5.com/csp/article/K93723284	A-F5-BIG--041122/1258
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.2					
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	https://support.f5.com/csp/article/K43024307	A-F5-BIG--041122/1260
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.1					
Incorrect Calculation	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. **CVE ID : CVE-2022-36795**	https://support.f5.com/csp/article/K52494562	A-F5-BIG--041122/1261
Missing Release of	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x	https://support.f5.com/c	A-F5-BIG--041122/1262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41624**	sp/article/K43024307	
Missing Release of Memory after Effective Lifetime	19-Oct-2022	7.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization. **CVE ID : CVE-2022-41832**	https://support.f5.com/csp/article/K10347453	A-F5-BIG--041122/1263
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1264
Product: big-ip_ssl_orchestrator					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1265
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1266
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Cleartext Transmission of Sensitive	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1268
Product: big-ip_webaccelerator					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1270
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied.	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41983		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1272
Product: big-ip_websafe					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1273
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1274
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1275
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Cleartext Transmission of Sensitive Information	19-Oct-2022	3.7	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions	https://support.f5.com/csp/article/K31523465	A-F5-BIG--041122/1276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied. **CVE ID : CVE-2022-41983**		
Product: big-iq_centralized_management					
Affected Version(s): 7.1.0					
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1277
Affected Version(s): From (including) 8.0.0 Up to (including) 8.2.0					
Uncontrolled Resource Consumption	19-Oct-2022	6.5	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource	https://support.f5.com/csp/article/K22505850	A-F5-BIG--041122/1278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			utilization, via undisclosed requests. **CVE ID : CVE-2022-41770**		
Product: nginx					
Affected Version(s): * Up to (excluding) 1.23.2					
Missing Release of Memory after Effective Lifetime	21-Oct-2022	7.5	A vulnerability was found in Nginx and classified as problematic. This issue affects some unknown processing of the file ngx_resolver.c of the component IPv4 Off Handler. The manipulation leads to memory leak. The attack may be initiated remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-211937 was assigned to this vulnerability. **CVE ID : CVE-2022-3638**	http://hg.nginx.org/nginx/rev/0422365794f7, https://github.com/nginx/nginx/commit/14341ce2377d38a268261e0fec65b6915ae6e95e	A-F5-NGIN-041122/1279
Affected Version(s): 1.23.0					
Out-of-bounds Write	19-Oct-2022	7.8	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to corrupt NGINX worker memory, resulting in its termination or potential	https://support.f5.com/csp/article/K81926432	A-F5-NGIN-041122/1280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other impact using a specially crafted audio or video file. The issue affects only NGINX products that are built with the ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41741**		
Out-of-bounds Write	19-Oct-2022	7.1	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted audio or video file. The issue affects only NGINX products that are built with the module ngx_http_mp4_module, when the mp4 directive	https://support.f5.com/csp/article/K28112382	A-F5-NGIN-041122/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41742**		
Affected Version(s): 1.23.1					
Out-of-bounds Write	19-Oct-2022	7.8	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to corrupt NGINX worker memory, resulting in its termination or potential other impact using a specially crafted audio or video file. The issue affects only NGINX products that are built with the ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video	https://support.f5.com/csp/article/K81926432	A-F5-NGIN-041122/1282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41741**		
Out-of-bounds Write	19-Oct-2022	7.1	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted audio or video file. The issue affects only NGINX products that are built with the module ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41742**	https://support.f5.com/csp/article/K28112382	A-F5-NGIN-041122/1283
Affected Version(s): From (including) 1.1.3 Up to (including) 1.22.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2022	7.8	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to corrupt NGINX worker memory, resulting in its termination or potential other impact using a specially crafted audio or video file. The issue affects only NGINX products that are built with the ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41741**	https://support.f5.com/csp/article/K81926432	A-F5-NGIN-041122/1284
Out-of-bounds Write	19-Oct-2022	7.1	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a	https://support.f5.com/csp/article/K28112382	A-F5-NGIN-041122/1285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the module ngx_http_mp4_module that might allow a local attacker to cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted audio or video file. The issue affects only NGINX products that are built with the module ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41742**		
Affected Version(s): From (including) r22 Up to (including) r27					
Out-of-bounds Write	19-Oct-2022	7.8	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to corrupt NGINX worker memory, resulting in its	https://support.f5.com/csp/article/K81926432	A-F5-NGIN-041122/1286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			termination or potential other impact using a specially crafted audio or video file. The issue affects only NGINX products that are built with the ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41741**		
Out-of-bounds Write	19-Oct-2022	7.1	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted audio or video file. The issue affects only NGINX products that are built with the module ngx_http_mp4_module,	https://support.f5.com/csp/article/K28112382	A-F5-NGIN-041122/1287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41742**		
Affected Version(s): r1					
Out-of-bounds Write	19-Oct-2022	7.8	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to corrupt NGINX worker memory, resulting in its termination or potential other impact using a specially crafted audio or video file. The issue affects only NGINX products that are built with the ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially	https://support.f5.com/csp/article/K81926432	A-F5-NGIN-041122/1288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted audio or video file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41741**		
Out-of-bounds Write	19-Oct-2022	7.1	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted audio or video file. The issue affects only NGINX products that are built with the module ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41742**	https://support.f5.com/csp/article/K28112382	A-F5-NGIN-041122/1289
Affected Version(s): r2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2022	7.8	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to corrupt NGINX worker memory, resulting in its termination or potential other impact using a specially crafted audio or video file. The issue affects only NGINX products that are built with the ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41741**	https://support.f5.com/csp/article/K81926432	A-F5-NGIN-041122/1290
Out-of-bounds Write	19-Oct-2022	7.1	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a	https://support.f5.com/csp/article/K28112382	A-F5-NGIN-041122/1291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the module ngx_http_mp4_module that might allow a local attacker to cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted audio or video file. The issue affects only NGINX products that are built with the module ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41742**		
Product: nginx_ingress_controller					
Affected Version(s): From (including) 1.9.0 Up to (including) 1.12.4					
Out-of-bounds Write	19-Oct-2022	7.8	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to corrupt NGINX worker memory,	https://support.f5.com/csp/article/K81926432	A-F5-NGIN-041122/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in its termination or potential other impact using a specially crafted audio or video file. The issue affects only NGINX products that are built with the ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41741**		
Out-of-bounds Write	19-Oct-2022	7.1	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted audio or video file. The issue affects only NGINX products that are built with the module	https://support.f5.com/csp/article/K28112382	A-F5-NGIN-041122/1293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41742**		
Out-of-bounds Write	19-Oct-2022	7	NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_hls_module that might allow a local attacker to corrupt NGINX worker memory, resulting in its crash or potential other impact using a specially crafted audio or video file. The issue affects only NGINX Plus when the hls directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_hls_module. **CVE ID : CVE-2022-41743**	https://support.f5.com/csp/article/K01112063	A-F5-NGIN-041122/1294
Affected Version(s): From (including) 2.0.0 Up to (including) 2.4.0					
Out-of-bounds Write	19-Oct-2022	7.8	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open	https://support.f5.com/c	A-F5-NGIN-041122/1295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to corrupt NGINX worker memory, resulting in its termination or potential other impact using a specially crafted audio or video file. The issue affects only NGINX products that are built with the ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41741**	sp/article/K81926432	
Out-of-bounds Write	19-Oct-2022	7.1	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module	https://support.f5.com/csp/article/K28112382	A-F5-NGIN-041122/1296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that might allow a local attacker to cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted audio or video file. The issue affects only NGINX products that are built with the module ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. **CVE ID : CVE-2022-41742**		
Out-of-bounds Write	19-Oct-2022	7	NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_hls_module that might allow a local attacker to corrupt NGINX worker memory, resulting in its crash or potential other impact using a specially crafted audio or video file. The issue affects only NGINX Plus when the hls directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger	https://support.f5.com/csp/article/K01112063	A-F5-NGIN-041122/1297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing of a specially crafted audio or video file with the module ngx_http_hls_module. **CVE ID : CVE-2022-41743**		
Product: nginx_plus					
Affected Version(s): From (including) r22 Up to (including) r27					
Out-of-bounds Write	19-Oct-2022	7	NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_hls_module that might allow a local attacker to corrupt NGINX worker memory, resulting in its crash or potential other impact using a specially crafted audio or video file. The issue affects only NGINX Plus when the hls directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_hls_module. **CVE ID : CVE-2022-41743**	https://support.f5.com/csp/article/K01112063	A-F5-NGIN-041122/1298
Product: njs					
Affected Version(s): 0.7.2					
Use After Free	28-Oct-2022	9.8	Nginx NJS v0.7.2 was discovered to contain a heap-use-after-free bug caused by illegal memory copy in the function	https://github.com/nginx/njs/commit/2ad0ea24a58d570634e09c2e58c3	A-F5-NJS-041122/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			njs_json_parse_iterator_call at njs_json.c. **CVE ID : CVE-2022-43286**	b314505eaa6a	
Affected Version(s): 0.7.4					
N/A	28-Oct-2022	7.5	Nginx NJS v0.7.4 was discovered to contain a segmentation violation in njs_promise_reaction_job. **CVE ID : CVE-2022-43285**	https://github.com/nginx/njs/issues/533	A-F5-NJS-041122/1300
Affected Version(s): From (including) 0.7.2 Up to (including) 0.7.4					
Out-of-bounds Read	28-Oct-2022	7.5	Nginx NJS v0.7.2 to v0.7.4 was discovered to contain a segmentation violation via njs_scope_valid_value at njs_scope.h. **CVE ID : CVE-2022-43284**	https://github.com/nginx/njs/issues/470	A-F5-NJS-041122/1301
Vendor: fatcatapps					
Product: analytics_cat					
Affected Version(s): * Up to (including) 1.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-2022	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) in Fatcat Apps Analytics Cat plugin <= 1.0.9 on WordPress. **CVE ID : CVE-2022-40311**	https://wordpress.org/plugins/analytics-cat/#developers, https://patchstack.com/database/vulnerability/analytics-cat/wordpress-analytics-cat-plugin-1-0-9-authenticate	A-FAT-ANAL-041122/1302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				d-stored-cross-site-scripting-xss-vulnerability?_s_id=cve	
Vendor: featherjs					
Product: feathers-sequelize					
Affected Version(s): * Up to (excluding) 6.3.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2022	9.8	Due to improper input validation in the Feathers js library, it is possible to perform a SQL injection attack on the back-end database, in case the feathers-sequelize package is used. **CVE ID : CVE-2022-2422**	https://csirt.divd.nl/cases/DIVD-2022-00020, https://csirt.divd.nl/cves/CVE-2022-2422	A-FEA-FEAT-041122/1303
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2022	9.8	Due to improper parameter filtering in the Feathers js library, which may ultimately lead to SQL injection **CVE ID : CVE-2022-29822**	https://csirt.divd.nl/cves/CVE-2022-29822/, https://csirt.divd.nl/cases/DIVD-2022-00020	A-FEA-FEAT-041122/1304
Improperly Controlled Modification of Object Prototype Attributes ('Prototype	26-Oct-2022	9.8	Feather-Sequalize cleanQuery method uses insecure recursive logic to filter unsupported keys from the query object. This results in a Remote Code Execution (RCE) with privileges of application. **CVE ID : CVE-2022-29823**	https://csirt.divd.nl/cases/DIVD-2022-00020, https://csirt.divd.nl/cves/CVE-2022-29823/	A-FEA-FEAT-041122/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pollution')					
Vendor: flutter					
Product: flutter					
Affected Version(s): * Up to (excluding) 3.3.3					
N/A	27-Oct-2022	9.8	The implementation of backslash parsing in the Dart URI class for versions prior to 2.18 and Flutter versions prior to 3.30 differs from the WhatWG URL standards. Dart uses the RFC 3986 syntax, which creates incompatibilities with the '\' characters in URIs, which can lead to auth bypass in webapps interpreting URIs. We recommend updating Dart or Flutter to mitigate the issue. **CVE ID : CVE-2022-3095**	https://github.com/dart-lang/sdk/blob/master/CHANGELOG.md#2182---2022-09-28	A-FLU-FLUT-041122/1306
Vendor: fluxcd					
Product: flux2					
Affected Version(s): From (including) 0.1.0 Up to (excluding) 0.35.0					
Improper Input Validation	22-Oct-2022	4.3	Flux is an open and extensible continuous delivery solution for Kubernetes. Versions prior to 0.35.0 are subject to a Denial of Service. Users that have permissions to change Fluxâ€™s objects, either through a Flux source or directly within a cluster, can provide invalid data to fields `.spec.interval` or `.spec.timeout` (and	https://github.com/fluxcd/flux2/security/advisories/GHSA-f4p5-x4vc-mh4v, https://github.com/kubernetes/apimachinery/issues/131	A-FLU-FLUX-041122/1307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			structured variations of these fields), causing the entire object type to stop being processed. This issue is patched in version 0.35.0. As a workaround, Admission controllers can be employed to restrict the values that can be used for fields `.spec.interval` and `.spec.timeout`, however upgrading to the latest versions is still the recommended mitigation. **CVE ID : CVE-2022-39272**		
Product: helm-controller					
Affected Version(s): 0.0.1					
Improper Input Validation	22-Oct-2022	4.3	Flux is an open and extensible continuous delivery solution for Kubernetes. Versions prior to 0.35.0 are subject to a Denial of Service. Users that have permissions to change Fluxâ€™s objects, either through a Flux source or directly within a cluster, can provide invalid data to fields `.spec.interval` or `.spec.timeout` (and structured variations of these fields), causing the entire object type to stop being processed. This issue is patched in version 0.35.0. As a workaround, Admission controllers can be employed to restrict the	https://github.com/fluxcd/flux2/security/advisories/GHSA-f4p5-x4vc-mh4v, https://github.com/kubernetes/apimachinery/issues/131	A-FLU-HELM-041122/1308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			values that can be used for fields `.spec.interval` and `.spec.timeout`, however upgrading to the latest versions is still the recommended mitigation. **CVE ID : CVE-2022-39272**		
Affected Version(s): From (including) 0.0.2 Up to (excluding) 0.24.0					
Improper Input Validation	22-Oct-2022	4.3	Flux is an open and extensible continuous delivery solution for Kubernetes. Versions prior to 0.35.0 are subject to a Denial of Service. Users that have permissions to change Fluxâ€™s objects, either through a Flux source or directly within a cluster, can provide invalid data to fields `.spec.interval` or `.spec.timeout` (and structured variations of these fields), causing the entire object type to stop being processed. This issue is patched in version 0.35.0. As a workaround, Admission controllers can be employed to restrict the values that can be used for fields `.spec.interval` and `.spec.timeout`, however upgrading to the latest versions is still the recommended mitigation. **CVE ID : CVE-2022-39272**	https://github.com/fluxcd/flux2/security/advisories/GHSA-f4p5-x4vc-mh4v, https://github.com/kubernetes/apimachinery/issues/131	A-FLU-HELM-041122/1309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: image-automation-controller					
Affected Version(s): From (including) 0.1.0 Up to (excluding) 0.26.0					
Improper Input Validation	22-Oct-2022	4.3	Flux is an open and extensible continuous delivery solution for Kubernetes. Versions prior to 0.35.0 are subject to a Denial of Service. Users that have permissions to change Fluxâ€™s objects, either through a Flux source or directly within a cluster, can provide invalid data to fields `.spec.interval` or `.spec.timeout` (and structured variations of these fields), causing the entire object type to stop being processed. This issue is patched in version 0.35.0. As a workaround, Admission controllers can be employed to restrict the values that can be used for fields `.spec.interval` and `.spec.timeout`, however upgrading to the latest versions is still the recommended mitigation. **CVE ID : CVE-2022-39272**	https://github.com/fluxcd/flux2/security/advisories/GHSA-f4p5-x4vc-mh4v, https://github.com/kubernetes/apimachinery/issues/131	A-FLU-IMAG-041122/1310
Product: image-reflector-controller					
Affected Version(s): From (including) 0.1.0 Up to (excluding) 0.22.0					
Improper Input Validation	22-Oct-2022	4.3	Flux is an open and extensible continuous delivery solution for Kubernetes. Versions prior to 0.35.0 are subject to a Denial of	https://github.com/fluxcd/flux2/security/advisories/GHSA-f4p5-x4vc-	A-FLU-IMAG-041122/1311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service. Users that have permissions to change Fluxâ€™s objects, either through a Flux source or directly within a cluster, can provide invalid data to fields `.spec.interval` or `.spec.timeout` (and structured variations of these fields), causing the entire object type to stop being processed. This issue is patched in version 0.35.0. As a workaround, Admission controllers can be employed to restrict the values that can be used for fields `.spec.interval` and `.spec.timeout`, however upgrading to the latest versions is still the recommended mitigation. **CVE ID : CVE-2022-39272**	mh4v, https://github.com/kubernetes/apimachinery/issues/131	
Product: kustomize-controller					
Affected Version(s): 0.0.1					
Improper Input Validation	22-Oct-2022	4.3	Flux is an open and extensible continuous delivery solution for Kubernetes. Versions prior to 0.35.0 are subject to a Denial of Service. Users that have permissions to change Fluxâ€™s objects, either through a Flux source or directly within a cluster, can provide invalid data to fields `.spec.interval` or `.spec.timeout` (and structured variations of	https://github.com/fluxcd/flux2/security/advisories/GHSA-f4p5-x4vc-mh4v, https://github.com/kubernetes/apimachinery/issues/131	A-FLU-KUST-041122/1312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these fields), causing the entire object type to stop being processed. This issue is patched in version 0.35.0. As a workaround, Admission controllers can be employed to restrict the values that can be used for fields `.spec.interval` and `.spec.timeout`, however upgrading to the latest versions is still the recommended mitigation. **CVE ID : CVE-2022-39272**		
Affected Version(s): From (including) 0.0.2 Up to (excluding) 0.29.0					
Improper Input Validation	22-Oct-2022	4.3	Flux is an open and extensible continuous delivery solution for Kubernetes. Versions prior to 0.35.0 are subject to a Denial of Service. Users that have permissions to change Fluxâ€™s objects, either through a Flux source or directly within a cluster, can provide invalid data to fields `.spec.interval` or `.spec.timeout` (and structured variations of these fields), causing the entire object type to stop being processed. This issue is patched in version 0.35.0. As a workaround, Admission controllers can be employed to restrict the values that can be used for fields `.spec.interval`	https://github.com/fluxcd/flux2/security/advisories/GHSA-f4p5-x4vc-mh4v, https://github.com/kubernetes/apimachinery/issues/131	A-FLU-KUST-041122/1313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and `.spec.timeout`, however upgrading to the latest versions is still the recommended mitigation. **CVE ID : CVE-2022-39272**		
Product: notification-controller					
Affected Version(s): 0.0.1					
Improper Input Validation	22-Oct-2022	4.3	Flux is an open and extensible continuous delivery solution for Kubernetes. Versions prior to 0.35.0 are subject to a Denial of Service. Users that have permissions to change Fluxâ€™s objects, either through a Flux source or directly within a cluster, can provide invalid data to fields `.spec.interval` or `.spec.timeout` (and structured variations of these fields), causing the entire object type to stop being processed. This issue is patched in version 0.35.0. As a workaround, Admission controllers can be employed to restrict the values that can be used for fields `.spec.interval` and `.spec.timeout`, however upgrading to the latest versions is still the recommended mitigation. **CVE ID : CVE-2022-39272**	https://github.com/fluxcd/flux2/security/advisories/GHSA-f4p5-x4vc-mh4v, https://github.com/kubernetes/apimachinery/issues/131	A-FLU-NOTI-041122/1314
Affected Version(s): From (including) 0.0.2 Up to (excluding) 0.27.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	22-Oct-2022	4.3	Flux is an open and extensible continuous delivery solution for Kubernetes. Versions prior to 0.35.0 are subject to a Denial of Service. Users that have permissions to change Fluxâ€™s objects, either through a Flux source or directly within a cluster, can provide invalid data to fields `.spec.interval` or `.spec.timeout` (and structured variations of these fields), causing the entire object type to stop being processed. This issue is patched in version 0.35.0. As a workaround, Admission controllers can be employed to restrict the values that can be used for fields `.spec.interval` and `.spec.timeout`, however upgrading to the latest versions is still the recommended mitigation. **CVE ID : CVE-2022-39272**	https://github.com/fluxcd/flux2/security/advisories/GHSA-f4p5-x4vc-mh4v, https://github.com/kubernetes/apimachinery/issues/131	A-FLU-NOTI-041122/1315
Product: source-controller					
Affected Version(s): 0.0.1					
Improper Input Validation	22-Oct-2022	4.3	Flux is an open and extensible continuous delivery solution for Kubernetes. Versions prior to 0.35.0 are subject to a Denial of Service. Users that have permissions to change Fluxâ€™s objects, either	https://github.com/fluxcd/flux2/security/advisories/GHSA-f4p5-x4vc-mh4v, https://github.com/kub	A-FLU-SOUR-041122/1316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a Flux source or directly within a cluster, can provide invalid data to fields `.spec.interval` or `.spec.timeout` (and structured variations of these fields), causing the entire object type to stop being processed. This issue is patched in version 0.35.0. As a workaround, Admission controllers can be employed to restrict the values that can be used for fields `.spec.interval` and `.spec.timeout`, however upgrading to the latest versions is still the recommended mitigation. **CVE ID : CVE-2022-39272**	ernetes/api machinery/issues/131	
Affected Version(s): From (including) 0.0.2 Up to (excluding) 0.30.0					
Improper Input Validation	22-Oct-2022	4.3	Flux is an open and extensible continuous delivery solution for Kubernetes. Versions prior to 0.35.0 are subject to a Denial of Service. Users that have permissions to change Fluxâ€™s objects, either through a Flux source or directly within a cluster, can provide invalid data to fields `.spec.interval` or `.spec.timeout` (and structured variations of these fields), causing the entire object type to stop being processed. This issue is patched in	https://github.com/fluxcd/flux2/security/advisories/GHSA-f4p5-x4vc-mh4v, https://github.com/kubernetes/api machinery/issues/131	A-FLU-SOUR-041122/1317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 0.35.0. As a workaround, Admission controllers can be employed to restrict the values that can be used for fields `.spec.interval` and `.spec.timeout`, however upgrading to the latest versions is still the recommended mitigation. **CVE ID : CVE-2022-39272**		
Vendor: Forgerock					
Product: access_management					
Affected Version(s): 7.1.0					
N/A	27-Oct-2022	6.5	An attacker can use the unrestricted LDAP queries to determine configuration entries **CVE ID : CVE-2022-24670**	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1318
Missing Authorization	27-Oct-2022	6.5	It may be possible to gain some details of the deployment through a well-crafted attack. This may allow that data to be used to probe internal network services. **CVE ID : CVE-2022-24669**	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1319
Affected Version(s): 6.5.1					
N/A	27-Oct-2022	6.5	An attacker can use the unrestricted LDAP queries to determine configuration entries **CVE ID : CVE-2022-24670**	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	27-Oct-2022	6.5	It may be possible to gain some details of the deployment through a well-crafted attack. This may allow that data to be used to probe internal network services. **CVE ID : CVE-2022-24669**	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1321
Affected Version(s): 6.5.3					
N/A	27-Oct-2022	6.5	An attacker can use the unrestricted LDAP queries to determine configuration entries **CVE ID : CVE-2022-24670**	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1322
Missing Authorization	27-Oct-2022	6.5	It may be possible to gain some details of the deployment through a well-crafted attack. This may allow that data to be used to probe internal network services. **CVE ID : CVE-2022-24669**	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1323
Affected Version(s): 6.5.4					
N/A	27-Oct-2022	6.5	An attacker can use the unrestricted LDAP queries to determine configuration entries **CVE ID : CVE-2022-24670**	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1324
Missing Authorization	27-Oct-2022	6.5	It may be possible to gain some details of the deployment through a well-crafted attack. This may allow that data to be used to probe internal network services.	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24669		
Affected Version(s): 7.1.1					
N/A	27-Oct-2022	6.5	An attacker can use the unrestricted LDAP queries to determine configuration entries **CVE ID : CVE-2022-24670**	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1326
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.0.7					
N/A	27-Oct-2022	6.5	An attacker can use the unrestricted LDAP queries to determine configuration entries **CVE ID : CVE-2022-24670**	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1327
Missing Authorization	27-Oct-2022	6.5	It may be possible to gain some details of the deployment through a well-crafted attack. This may allow that data to be used to probe internal network services. **CVE ID : CVE-2022-24669**	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1328
Affected Version(s): From (including) 6.5.0 Up to (including) 6.5.0.2					
N/A	27-Oct-2022	6.5	An attacker can use the unrestricted LDAP queries to determine configuration entries **CVE ID : CVE-2022-24670**	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1329
Missing Authorization	27-Oct-2022	6.5	It may be possible to gain some details of the deployment through a well-crafted attack. This may allow that data to be used to probe internal network services.	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24669		
Affected Version(s): From (including) 6.5.2.1 Up to (including) 6.5.2.3					
N/A	27-Oct-2022	6.5	An attacker can use the unrestricted LDAP queries to determine configuration entries **CVE ID : CVE-2022-24670**	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1331
Missing Authorization	27-Oct-2022	6.5	It may be possible to gain some details of the deployment through a well-crafted attack. This may allow that data to be used to probe internal network services. **CVE ID : CVE-2022-24669**	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1332
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.2					
N/A	27-Oct-2022	6.5	An attacker can use the unrestricted LDAP queries to determine configuration entries **CVE ID : CVE-2022-24670**	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1333
Missing Authorization	27-Oct-2022	6.5	It may be possible to gain some details of the deployment through a well-crafted attack. This may allow that data to be used to probe internal network services. **CVE ID : CVE-2022-24669**	https://backstage.forgerock.com/knowledge/kb/article/a90639318	A-FOR-ACCE-041122/1334
Vendor: Fortinet					
Product: fortiproxy					
Affected Version(s): 7.2.0					
Missing Authentic	18-Oct-2022	9.8	An authentication bypass using an alternate path	https://fortiguard.com/p	A-FOR-FORT-041122/1335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation for Critical Function			or channel [CWE-288] in Fortinet FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0 allows an unauthenticated atttacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests. **CVE ID : CVE-2022-40684**	sirt/FG-IR-22-377	
Access of Uninitialized Pointer	18-Oct-2022	7.5	A access of uninitialized pointer in Fortinet FortiOS version 7.2.0, 7.0.0 through 7.0.5, 6.4.0 through 6.4.8, 6.2.0 through 6.2.10, 6.0.x, FortiProxy version 7.0.0 through 7.0.4, 2.0.0 through 2.0.9, 1.2.x allows a remote unauthenticated or authenticated attacker to crash the sslvpn daemon via an HTTP GET request. **CVE ID : CVE-2022-29055**	https://fortiguard.com/psirt/FG-IR-22-086	A-FOR-FORT-041122/1336
Affected Version(s): From (including) 1.2.6 Up to (excluding) 1.2.13					
Access of Uninitialized Pointer	18-Oct-2022	7.5	A access of uninitialized pointer in Fortinet FortiOS version 7.2.0, 7.0.0 through 7.0.5, 6.4.0 through 6.4.8, 6.2.0 through 6.2.10, 6.0.x, FortiProxy version 7.0.0	https://fortiguard.com/psirt/FG-IR-22-086	A-FOR-FORT-041122/1337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 7.0.4, 2.0.0 through 2.0.9, 1.2.x allows a remote unauthenticated or authenticated attacker to crash the sslvpn daemon via an HTTP GET request. **CVE ID : CVE-2022-29055**		
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.0.10					
Access of Uninitialized Pointer	18-Oct-2022	7.5	A access of uninitialized pointer in Fortinet FortiOS version 7.2.0, 7.0.0 through 7.0.5, 6.4.0 through 6.4.8, 6.2.0 through 6.2.10, 6.0.x, FortiProxy version 7.0.0 through 7.0.4, 2.0.0 through 2.0.9, 1.2.x allows a remote unauthenticated or authenticated attacker to crash the sslvpn daemon via an HTTP GET request. **CVE ID : CVE-2022-29055**	https://fortiguard.com/psirt/FG-IR-22-086	A-FOR-FORT-041122/1338
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.7					
Missing Authentication for Critical Function	18-Oct-2022	9.8	An authentication bypass using an alternate path or channel [CWE-288] in Fortinet FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0 allows an unauthenticated atttacker to perform operations on the	https://fortiguard.com/psirt/FG-IR-22-377	A-FOR-FORT-041122/1339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrative interface via specially crafted HTTP or HTTPS requests. **CVE ID : CVE-2022-40684**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	A access of uninitialized pointer in Fortinet FortiOS version 7.2.0, 7.0.0 through 7.0.5, 6.4.0 through 6.4.8, 6.2.0 through 6.2.10, 6.0.x, FortiProxy version 7.0.0 through 7.0.4, 2.0.0 through 2.0.9, 1.2.x allows a remote unauthenticated or authenticated attacker to crash the sslvpn daemon via an HTTP GET request. **CVE ID : CVE-2022-29055**	https://fortiguard.com/psirt/FG-IR-22-086	A-FOR-FORT-041122/1340
Product: fortiswitchmanager					
Affected Version(s): 7.2.0					
Missing Authentication for Critical Function	18-Oct-2022	9.8	An authentication bypass using an alternate path or channel [CWE-288] in Fortinet FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0 allows an unauthenticated atttacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests.	https://fortiguard.com/psirt/FG-IR-22-377	A-FOR-FORT-041122/1341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40684		
Affected Version(s): 7.0.0					
Missing Authentication for Critical Function	18-Oct-2022	9.8	An authentication bypass using an alternate path or channel [CWE-288] in Fortinet FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0 allows an unauthenticated atttacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests. **CVE ID : CVE-2022-40684**	https://fortiguard.com/psirt/FG-IR-22-377	A-FOR-FORT-041122/1342
Product: fortitester					
Affected Version(s): From (including) 2.3.0 Up to (excluding) 3.9.2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Oct-2022	9.8	An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in Telnet login components of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an unauthenticated remote attacker to execute arbitrary command in the underlying shell.	https://fortiguard.com/psirt/FG-IR-22-237	A-FOR-FORT-041122/1343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33872		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Oct-2022	9.8	An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in Console login components of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an unauthenticated attacker to execute arbitrary command in the underlying shell. **CVE ID : CVE-2022-33873**	https://fortiguard.com/psirt/FG-IR-22-237	A-FOR-FORT-041122/1344
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Oct-2022	9.8	An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in SSH login components of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an unauthenticated remote attacker to execute arbitrary command in the underlying shell. **CVE ID : CVE-2022-33874**	https://fortiguard.com/psirt/FG-IR-22-237	A-FOR-FORT-041122/1345
Improper Restriction of Excessive Authentic	18-Oct-2022	9.8	An improper restriction of excessive authentication attempts vulnerability [CWE-307] in FortiTester Telnet	https://fortiguard.com/psirt/FG-IR-22-244	A-FOR-FORT-041122/1346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation Attempts			port 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an unauthenticated attacker to guess the credentials of an admin user via a brute force attack. **CVE ID : CVE-2022-35846**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Oct-2022	7.2	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the management interface of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to commands of the certificate import feature. **CVE ID : CVE-2022-35844**	https://fortiguard.com/psirt/FG-IR-22-247	A-FOR-FORT-041122/1347
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Oct-2022	9.8	An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in Telnet login components of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an unauthenticated remote attacker to	https://fortiguard.com/psirt/FG-IR-22-237	A-FOR-FORT-041122/1348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary command in the underlying shell. **CVE ID : CVE-2022-33872**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Oct-2022	9.8	An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in Console login components of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an unauthenticated attacker to execute arbitrary command in the underlying shell. **CVE ID : CVE-2022-33873**	https://fortiguard.com/psirt/FG-IR-22-237	A-FOR-FORT-041122/1349
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Oct-2022	9.8	An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in SSH login components of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an unauthenticated remote attacker to execute arbitrary command in the underlying shell. **CVE ID : CVE-2022-33874**	https://fortiguard.com/psirt/FG-IR-22-237	A-FOR-FORT-041122/1350
Improper Restrictio	18-Oct-2022	9.8	An improper restriction of excessive	https://fortiguard.com/p	A-FOR-FORT-041122/1351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n of Excessive Authentication Attempts			authentication attempts vulnerability [CWE-307] in FortiTester Telnet port 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an unauthenticated attacker to guess the credentials of an admin user via a brute force attack. **CVE ID : CVE-2022-35846**	sirt/FG-IR-22-244	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Oct-2022	7.2	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the management interface of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to commands of the certificate import feature. **CVE ID : CVE-2022-35844**	https://fortiguard.com/psirt/FG-IR-22-247	A-FOR-FORT-041122/1352
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.1.1					
Improper Neutralization of Special Elements used in an OS Command ('OS	18-Oct-2022	9.8	An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in Telnet login components of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0,	https://fortiguard.com/psirt/FG-IR-22-237	A-FOR-FORT-041122/1353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			7.0.0 through 7.1.0 may allow an unauthenticated remote attacker to execute arbitrary command in the underlying shell. **CVE ID : CVE-2022-33872**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Oct-2022	9.8	An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in Console login components of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an unauthenticated attacker to execute arbitrary command in the underlying shell. **CVE ID : CVE-2022-33873**	https://fortiguard.com/psirt/FG-IR-22-237	A-FOR-FORT-041122/1354
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Oct-2022	9.8	An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in SSH login components of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an unauthenticated remote attacker to execute arbitrary command in the underlying shell.	https://fortiguard.com/psirt/FG-IR-22-237	A-FOR-FORT-041122/1355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33874		
Improper Restriction of Excessive Authentication Attempts	18-Oct-2022	9.8	An improper restriction of excessive authentication attempts vulnerability [CWE-307] in FortiTester Telnet port 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an unauthenticated attacker to guess the credentials of an admin user via a brute force attack. **CVE ID : CVE-2022-35846**	https://fortiguard.com/psirt/FG-IR-22-244	A-FOR-FORT-041122/1356
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Oct-2022	7.2	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the management interface of FortiTester 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to commands of the certificate import feature. **CVE ID : CVE-2022-35844**	https://fortiguard.com/psirt/FG-IR-22-247	A-FOR-FORT-041122/1357
Vendor: free5gc					
Product: free5gc					
Affected Version(s): 3.2.1					
Missing Authentication for	25-Oct-2022	7.5	Free5gc v3.2.1 is vulnerable to Information disclosure.	N/A	A-FRE-FREE-041122/1358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			**CVE ID : CVE-2022-38870**		
N/A	24-Oct-2022	5.5	In free5GC 3.2.1, a malformed NGAP message can crash the AMF and NGAP decoders via an index-out-of-range panic in aper.GetBitString. **CVE ID : CVE-2022-43677**	N/A	A-FRE-FREE-041122/1359
Vendor: fujielectric					
Product: d300win					
Affected Version(s): * Up to (excluding) 3.7.1.17					
Out-of-bounds Write	19-Oct-2022	9.1	Fuji Electric D300win prior to version 3.7.1.17 is vulnerable to a write-what-where condition, which could allow an attacker to overwrite program memory to manipulate the flow of information. **CVE ID : CVE-2022-1523**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-05	A-FUJ-D300-041122/1360
Out-of-bounds Read	19-Oct-2022	7.5	Fuji Electric D300win prior to version 3.7.1.17 is vulnerable to an out-of-bounds read, which could allow an attacker to leak sensitive data from the process memory. **CVE ID : CVE-2022-1738**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-05	A-FUJ-D300-041122/1361
Vendor: garage_management_system_project					
Product: garage_management_system					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2022	5.4	A stored cross-site scripting (XSS) vulnerability in Garage Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the categoriesName parameter in createCategories.php. **CVE ID : CVE-2022-41358**	N/A	A-GAR-GARA-041122/1362
Vendor: genivi					
Product: diagnostic_log_and_trace					
Affected Version(s): * Up to (including) 2.18.8					
Out-of-bounds Read	25-Oct-2022	5.5	An issue was discovered in Connected Vehicle Systems Alliance (COVESA) dlt-daemon through 2.18.8. Due to a faulty DLT file parser, a crafted DLT file that crashes the process can be created. This is due to missing validation checks. There is a heap-based buffer over-read of one byte. **CVE ID : CVE-2022-39836**	https://seclists.org/fulldisclosure/2022/Sep/24, https://sec-consult.com/vulnerability-lab/advisory/multiple-memory-corruption-vulnerabilities-in-covesa-dlt-daemon/	A-GEN-DIAG-041122/1363
NULL Pointer Dereference	25-Oct-2022	5.5	An issue was discovered in Connected Vehicle Systems Alliance (COVESA) dlt-daemon through 2.18.8. Due to a faulty DLT file parser, a crafted DLT file that crashes the process can be created. This is due to missing validation	https://seclists.org/fulldisclosure/2022/Sep/24, https://sec-consult.com/vulnerability-lab/advisory/multiple-	A-GEN-DIAG-041122/1364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checks. There is a NULL pointer dereference, **CVE ID : CVE-2022-39837**	memory-corruption-vulnerabilities-in-covesa-dlt-daemon/	
Vendor: Get-simple					
Product: getsimple_cms					
Affected Version(s): 3.3.16					
N/A	18-Oct-2022	9.8	GetSimple CMS v3.3.16 was discovered to contain a remote code execution (RCE) vulnerability via the edited_file parameter in admin/theme-edit.php. **CVE ID : CVE-2022-41544**	N/A	A-GET-GETS-041122/1365
Vendor: Getkirby					
Product: Kirby					
Affected Version(s): * Up to (excluding) 3.5.8.2					
Exposure of Resource to Wrong Sphere	25-Oct-2022	5.3	Kirby is a Content Management System. Prior to versions 3.5.8.2, 3.6.6.2, 3.7.5.1, and 3.8.1, a user enumeration vulnerability affects all Kirby sites with user accounts unless Kirby's API and Panel are disabled in the config. It can only be exploited for targeted attacks because the attack does not scale to brute force. The problem has been patched in Kirby 3.5.8.2, Kirby 3.6.6.2, Kirby 3.7.5.1, and Kirby 3.8.1. In all of the mentioned releases, the maintainers	https://github.com/getkirby/kirby/security/advisories/GHSA-c27j-76xg-6x4f	A-GET-KIRB-041122/1366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have rewritten the affected code so that the delay is also inserted after the brute force limit is reached. **CVE ID : CVE-2022-39315**		
Improper Restriction of Excessive Authentication Attempts	24-Oct-2022	3.7	Kirby is a flat-file CMS. In versions prior to 3.5.8.2, 3.6.6.2, 3.7.5.1, and 3.8.1, Kirby is subject to user enumeration due to Improper Restriction of Excessive Authentication Attempts. This vulnerability affects you only if you are using the `code` or `password-reset` auth method with the `auth.methods` option or if you have enabled the `debug` option in production. By using two or more IP addresses and multiple login attempts, valid user accounts will lock, but invalid accounts will not, leading to account enumeration. This issue has been patched in versions 3.5.8.2, 3.6.6.2, 3.7.5.1, and 3.8.1. If you cannot update immediately, you can work around the issue by setting the `auth.methods` option to `password`, which disables the code-based login and password reset forms.	https://github.com/getkirby/kirby/security/advisories/GHSA-43qq-qw4x-28f8	A-GET-KIRB-041122/1367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39314		
Affected Version(s): 3.8.0					
Exposure of Resource to Wrong Sphere	25-Oct-2022	5.3	Kirby is a Content Management System. Prior to versions 3.5.8.2, 3.6.6.2, 3.7.5.1, and 3.8.1, a user enumeration vulnerability affects all Kirby sites with user accounts unless Kirby's API and Panel are disabled in the config. It can only be exploited for targeted attacks because the attack does not scale to brute force. The problem has been patched in Kirby 3.5.8.2, Kirby 3.6.6.2, Kirby 3.7.5.1, and Kirby 3.8.1. In all of the mentioned releases, the maintainers have rewritten the affected code so that the delay is also inserted after the brute force limit is reached. **CVE ID : CVE-2022-39315**	https://github.com/getkirby/kirby/security/advisories/GHSA-c27j-76xg-6x4f	A-GET-KIRB-041122/1368
Improper Restriction of Excessive Authentication Attempts	24-Oct-2022	3.7	Kirby is a flat-file CMS. In versions prior to 3.5.8.2, 3.6.6.2, 3.7.5.1, and 3.8.1, Kirby is subject to user enumeration due to Improper Restriction of Excessive Authentication Attempts. This vulnerability affects you only if you are using the `code` or `password-reset` auth method with the `auth.methods`	https://github.com/getkirby/kirby/security/advisories/GHSA-43qq-qw4x-28f8	A-GET-KIRB-041122/1369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			option or if you have enabled the `debug` option in production. By using two or more IP addresses and multiple login attempts, valid user accounts will lock, but invalid accounts will not, leading to account enumeration. This issue has been patched in versions 3.5.8.2, 3.6.6.2, 3.7.5.1, and 3.8.1. If you cannot update immediately, you can work around the issue by setting the `auth.methods` option to `password`, which disables the code-based login and password reset forms. **CVE ID : CVE-2022-39314**		
Affected Version(s): From (including) 3.6.0 Up to (excluding) 3.6.6.2					
Exposure of Resource to Wrong Sphere	25-Oct-2022	5.3	Kirby is a Content Management System. Prior to versions 3.5.8.2, 3.6.6.2, 3.7.5.1, and 3.8.1, a user enumeration vulnerability affects all Kirby sites with user accounts unless Kirby's API and Panel are disabled in the config. It can only be exploited for targeted attacks because the attack does not scale to brute force. The problem has been patched in Kirby 3.5.8.2, Kirby 3.6.6.2, Kirby 3.7.5.1, and Kirby 3.8.1.	https://github.com/getkirby/kirby/security/advisories/GHSA-c27j-76xg-6x4f	A-GET-KIRB-041122/1370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			In all of the mentioned releases, the maintainers have rewritten the affected code so that the delay is also inserted after the brute force limit is reached. **CVE ID : CVE-2022-39315**		
Improper Restriction of Excessive Authentication Attempts	24-Oct-2022	3.7	Kirby is a flat-file CMS. In versions prior to 3.5.8.2, 3.6.6.2, 3.7.5.1, and 3.8.1, Kirby is subject to user enumeration due to Improper Restriction of Excessive Authentication Attempts. This vulnerability affects you only if you are using the `code` or `password-reset` auth method with the `auth.methods` option or if you have enabled the `debug` option in production. By using two or more IP addresses and multiple login attempts, valid user accounts will lock, but invalid accounts will not, leading to account enumeration. This issue has been patched in versions 3.5.8.2, 3.6.6.2, 3.7.5.1, and 3.8.1. If you cannot update immediately, you can work around the issue by setting the `auth.methods` option to `password`, which disables the code-based	https://github.com/getkirby/kirby/security/advisories/GHSA-43qq-qw4x-28f8	A-GET-KIRB-041122/1371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			login and password reset forms. **CVE ID : CVE-2022-39314**		
Affected Version(s): From (including) 3.7.0 Up to (excluding) 3.7.5.1					
Exposure of Resource to Wrong Sphere	25-Oct-2022	5.3	Kirby is a Content Management System. Prior to versions 3.5.8.2, 3.6.6.2, 3.7.5.1, and 3.8.1, a user enumeration vulnerability affects all Kirby sites with user accounts unless Kirby's API and Panel are disabled in the config. It can only be exploited for targeted attacks because the attack does not scale to brute force. The problem has been patched in Kirby 3.5.8.2, Kirby 3.6.6.2, Kirby 3.7.5.1, and Kirby 3.8.1. In all of the mentioned releases, the maintainers have rewritten the affected code so that the delay is also inserted after the brute force limit is reached. **CVE ID : CVE-2022-39315**	https://github.com/getkirby/kirby/security/advisories/GHSA-c27j-76xg-6x4f	A-GET-KIRB-041122/1372
Improper Restriction of Excessive Authentication Attempts	24-Oct-2022	3.7	Kirby is a flat-file CMS. In versions prior to 3.5.8.2, 3.6.6.2, 3.7.5.1, and 3.8.1, Kirby is subject to user enumeration due to Improper Restriction of Excessive Authentication Attempts. This vulnerability affects you only if you are using the	https://github.com/getkirby/kirby/security/advisories/GHSA-43qq-qw4x-28f8	A-GET-KIRB-041122/1373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`code` or `password-reset` auth method with the `auth.methods` option or if you have enabled the `debug` option in production. By using two or more IP addresses and multiple login attempts, valid user accounts will lock, but invalid accounts will not, leading to account enumeration. This issue has been patched in versions 3.5.8.2, 3.6.6.2, 3.7.5.1, and 3.8.1. If you cannot update immediately, you can work around the issue by setting the `auth.methods` option to `password`, which disables the code-based login and password reset forms. **CVE ID : CVE-2022-39314**		
Vendor: gin-vue-admin_project					
Product: gin-vue-admin					
Affected Version(s): * Up to (excluding) 2.5.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Oct-2022	7.5	Gin-vue-admin is a backstage management system based on vue and gin, which separates the front and rear of the full stack. Gin-vue-admin prior to 2.5.4 is vulnerable to path traversal, which leads to file upload vulnerabilities. Version 2.5.4 contains a patch for	https://github.com/flipped-aurora/gin-vue-admin/security/advisories/GHSA-7gc4-r5jr-9hxv, https://github.com/flipp	A-GIN-GIN--041122/1374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this issue. There are no workarounds aside from upgrading to a patched version. **CVE ID : CVE-2022-39345**	ed-aurora/gin-vue-admin/pull/1264	
Affected Version(s): * Up to (excluding) 2.5.4b					
Unrestricted Upload of File with Dangerous Type	24-Oct-2022	9.8	Gin-vue-admin is a backstage management system based on vue and gin, which separates the front and rear of the full stack. Versions prior to 2.5.4 contain a file upload ability. The affected code fails to validate fileMd5 and fileName parameters, resulting in an arbitrary file being read. This issue is patched in 2.5.4b. There are no known workarounds. **CVE ID : CVE-2022-39305**	https://github.com/flipped-aurora/gin-vue-admin/security/advisories/GHSA-wrmq-4v4c-gxp2	A-GIN-GIN--041122/1375
Affected Version(s): From (including) 2.5.1 Up to (including) 2.5.3b					
Unrestricted Upload of File with Dangerous Type	17-Oct-2022	9	In "Gin-Vue-Admin", versions v2.5.1 through v2.5.3b are vulnerable to Unrestricted File Upload that leads to execution of javascript code, through the "Compress Upload" functionality to the Media Library. When an admin user views the uploaded file, a low privilege attacker will get access to the admin's cookie leading to account takeover.	N/A	A-GIN-GIN--041122/1376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32176		
Vendor: Git-scm					
Product: git					
Affected Version(s): * Up to (excluding) 2.30.6					
Out-of-bounds Write	19-Oct-2022	8.8	Git is an open source, scalable, distributed revision control system. `git shell` is a restricted login shell that can be used to implement Git's push/pull functionality via SSH. In versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4, the function that splits the command arguments into an array improperly uses an `int` to represent the number of entries in the array, allowing a malicious actor to intentionally overflow the return value, leading to arbitrary heap writes. Because the resulting array is then passed to `execv()`, it is possible to leverage this attack to gain remote code execution on a victim machine. Note that a victim must first allow access to `git shell` as a login shell in order to be vulnerable to this attack. This problem is patched in versions 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 and users are advised to upgrade to the latest	https://github.com/git/git/security/advisories/GHSA-rjr6-wcq6-83p6	A-GIT-GIT-041122/1377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version. Disabling `git shell` access via remote logins is a viable short-term workaround. **CVE ID : CVE-2022-39260**		
Improper Link Resolution Before File Access ('Link Following')	19-Oct-2022	5.5	Git is an open source, scalable, distributed revision control system. Versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 are subject to exposure of sensitive information to a malicious actor. When performing a local clone (where the source and target of the clone are on the same volume), Git copies the contents of the source's `$GIT_DIR/objects` directory into the destination by either creating hardlinks to the source contents, or copying them (if hardlinks are disabled via `--no-hardlinks`). A malicious actor could convince a victim to clone a repository with a symbolic link pointing at sensitive information on the victim's machine. This can be done either by having the victim clone a malicious repository on the same machine, or having them clone a malicious repository embedded as	https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	A-GIT-GIT-041122/1378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a bare repository via a submodule from any source, provided they clone with the `--recurse-submodules` option. Git does not create symbolic links in the `$GIT_DIR/objects` directory. The problem has been patched in the versions published on 2022-10-18, and backported to v2.30.x. Potential workarounds: Avoid cloning untrusted repositories using the `--local` optimization when on a shared machine, either by passing the `--no-local` option to `git clone` or cloning from a URL that uses the `file://` scheme. Alternatively, avoid cloning repositories from untrusted sources with `--recurse-submodules` or run `git config --global protocol.file.allow user`. **CVE ID : CVE-2022-39253**		
Affected Version(s): 2.38.0					
Out-of-bounds Write	19-Oct-2022	8.8	Git is an open source, scalable, distributed revision control system. `git shell` is a restricted login shell that can be used to implement Git's push/pull functionality via SSH. In versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4, the	https://github.com/git/git/security/advisories/GHSA-rjr6-wcq6-83p6	A-GIT-GIT-041122/1379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function that splits the command arguments into an array improperly uses an `int` to represent the number of entries in the array, allowing a malicious actor to intentionally overflow the return value, leading to arbitrary heap writes. Because the resulting array is then passed to `execv()`, it is possible to leverage this attack to gain remote code execution on a victim machine. Note that a victim must first allow access to `git shell` as a login shell in order to be vulnerable to this attack. This problem is patched in versions 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 and users are advised to upgrade to the latest version. Disabling `git shell` access via remote logins is a viable short-term workaround. **CVE ID : CVE-2022-39260**		
Improper Link Resolution Before File Access ('Link Following')	19-Oct-2022	5.5	Git is an open source, scalable, distributed revision control system. Versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 are subject to exposure of sensitive information to a malicious actor. When	https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	A-GIT-GIT-041122/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performing a local clone (where the source and target of the clone are on the same volume), Git copies the contents of the source's `$GIT_DIR/objects` directory into the destination by either creating hardlinks to the source contents, or copying them (if hardlinks are disabled via `--no-hardlinks`). A malicious actor could convince a victim to clone a repository with a symbolic link pointing at sensitive information on the victim's machine. This can be done either by having the victim clone a malicious repository on the same machine, or having them clone a malicious repository embedded as a bare repository via a submodule from any source, provided they clone with the `--recurse-submodules` option. Git does not create symbolic links in the `$GIT_DIR/objects` directory. The problem has been patched in the versions published on 2022-10-18, and backported to v2.30.x. Potential workarounds: Avoid cloning untrusted repositories using the `--local` optimization when		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on a shared machine, either by passing the `--no-local` option to `git clone` or cloning from a URL that uses the `file://` scheme. Alternatively, avoid cloning repositories from untrusted sources with `--recurse-submodules` or run `git config --global protocol.file.allow user`. **CVE ID : CVE-2022-39253**		
Affected Version(s): From (including) 2.31.0 Up to (excluding) 2.31.5					
Out-of-bounds Write	19-Oct-2022	8.8	Git is an open source, scalable, distributed revision control system. `git shell` is a restricted login shell that can be used to implement Git's push/pull functionality via SSH. In versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4, the function that splits the command arguments into an array improperly uses an `int` to represent the number of entries in the array, allowing a malicious actor to intentionally overflow the return value, leading to arbitrary heap writes. Because the resulting array is then passed to `execv()`, it is possible to leverage this attack to gain remote code execution on a victim machine. Note that a	https://github.com/git/git/security/advisories/GHSA-rjr6-wcq6-83p6	A-GIT-GIT-041122/1381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must first allow access to `git shell` as a login shell in order to be vulnerable to this attack. This problem is patched in versions 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 and users are advised to upgrade to the latest version. Disabling `git shell` access via remote logins is a viable short-term workaround. **CVE ID : CVE-2022-39260**		
Improper Link Resolution Before File Access ('Link Following')	19-Oct-2022	5.5	Git is an open source, scalable, distributed revision control system. Versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 are subject to exposure of sensitive information to a malicious actor. When performing a local clone (where the source and target of the clone are on the same volume), Git copies the contents of the source's `$GIT_DIR/objects` directory into the destination by either creating hardlinks to the source contents, or copying them (if hardlinks are disabled via `--no-hardlinks`). A malicious actor could convince a victim to clone a repository with a	https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	A-GIT-GIT-041122/1382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			symbolic link pointing at sensitive information on the victim's machine. This can be done either by having the victim clone a malicious repository on the same machine, or having them clone a malicious repository embedded as a bare repository via a submodule from any source, provided they clone with the `--recurse-submodules` option. Git does not create symbolic links in the `$GIT_DIR/objects` directory. The problem has been patched in the versions published on 2022-10-18, and backported to v2.30.x. Potential workarounds: Avoid cloning untrusted repositories using the `--local` optimization when on a shared machine, either by passing the `--no-local` option to `git clone` or cloning from a URL that uses the `file://` scheme. Alternatively, avoid cloning repositories from untrusted sources with `--recurse-submodules` or run `git config --global protocol.file.allow user`. **CVE ID : CVE-2022-39253**		
Affected Version(s): From (including) 2.32.0 Up to (excluding) 2.32.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2022	8.8	Git is an open source, scalable, distributed revision control system. `git shell` is a restricted login shell that can be used to implement Git's push/pull functionality via SSH. In versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4, the function that splits the command arguments into an array improperly uses an `int` to represent the number of entries in the array, allowing a malicious actor to intentionally overflow the return value, leading to arbitrary heap writes. Because the resulting array is then passed to `execv()`, it is possible to leverage this attack to gain remote code execution on a victim machine. Note that a victim must first allow access to `git shell` as a login shell in order to be vulnerable to this attack. This problem is patched in versions 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 and users are advised to upgrade to the latest version. Disabling `git shell` access via remote logins is a viable short-term workaround.	https://github.com/git/git/security/advisories/GHSA-rjr6-wcq6-83p6	A-GIT-GIT-041122/1383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39260		
Improper Link Resolution Before File Access ('Link Following')	19-Oct-2022	5.5	Git is an open source, scalable, distributed revision control system. Versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 are subject to exposure of sensitive information to a malicious actor. When performing a local clone (where the source and target of the clone are on the same volume), Git copies the contents of the source's `$GIT_DIR/objects` directory into the destination by either creating hardlinks to the source contents, or copying them (if hardlinks are disabled via `--no-hardlinks`). A malicious actor could convince a victim to clone a repository with a symbolic link pointing at sensitive information on the victim's machine. This can be done either by having the victim clone a malicious repository on the same machine, or having them clone a malicious repository embedded as a bare repository via a submodule from any source, provided they clone with the `--recurse-submodules` option. Git	https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	A-GIT-GIT-041122/1384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not create symbolic links in the `$GIT_DIR/objects` directory. The problem has been patched in the versions published on 2022-10-18, and backported to v2.30.x. Potential workarounds: Avoid cloning untrusted repositories using the `--local` optimization when on a shared machine, either by passing the `--no-local` option to `git clone` or cloning from a URL that uses the `file://` scheme. Alternatively, avoid cloning repositories from untrusted sources with `--recurse-submodules` or run `git config --global protocol.file.allow user`. **CVE ID : CVE-2022-39253**		
Affected Version(s): From (including) 2.33.0 Up to (excluding) 2.33.5					
Out-of-bounds Write	19-Oct-2022	8.8	Git is an open source, scalable, distributed revision control system. `git shell` is a restricted login shell that can be used to implement Git's push/pull functionality via SSH. In versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4, the function that splits the command arguments into an array improperly uses an `int` to represent the number of entries in	https://github.com/git/git/security/advisories/GHSA-rjr6-wcq6-83p6	A-GIT-GIT-041122/1385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the array, allowing a malicious actor to intentionally overflow the return value, leading to arbitrary heap writes. Because the resulting array is then passed to `execv()`, it is possible to leverage this attack to gain remote code execution on a victim machine. Note that a victim must first allow access to `git shell` as a login shell in order to be vulnerable to this attack. This problem is patched in versions 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 and users are advised to upgrade to the latest version. Disabling `git shell` access via remote logins is a viable short-term workaround. **CVE ID : CVE-2022-39260**		
Improper Link Resolution Before File Access ('Link Following')	19-Oct-2022	5.5	Git is an open source, scalable, distributed revision control system. Versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 are subject to exposure of sensitive information to a malicious actor. When performing a local clone (where the source and target of the clone are on the same volume), Git copies the contents of the	https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	A-GIT-GIT-041122/1386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			source's `$GIT_DIR/objects` directory into the destination by either creating hardlinks to the source contents, or copying them (if hardlinks are disabled via `--no-hardlinks`). A malicious actor could convince a victim to clone a repository with a symbolic link pointing at sensitive information on the victim's machine. This can be done either by having the victim clone a malicious repository on the same machine, or having them clone a malicious repository embedded as a bare repository via a submodule from any source, provided they clone with the `--recurse-submodules` option. Git does not create symbolic links in the `$GIT_DIR/objects` directory. The problem has been patched in the versions published on 2022-10-18, and backported to v2.30.x. Potential workarounds: Avoid cloning untrusted repositories using the `--local` optimization when on a shared machine, either by passing the `--no-local` option to `git clone` or cloning from a URL that uses the `file://`		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scheme. Alternatively, avoid cloning repositories from untrusted sources with `--recurse-submodules` or run `git config --global protocol.file.allow user`. **CVE ID : CVE-2022-39253**		
Affected Version(s): From (including) 2.34.0 Up to (excluding) 2.34.5					
Out-of-bounds Write	19-Oct-2022	8.8	Git is an open source, scalable, distributed revision control system. `git shell` is a restricted login shell that can be used to implement Git's push/pull functionality via SSH. In versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4, the function that splits the command arguments into an array improperly uses an `int` to represent the number of entries in the array, allowing a malicious actor to intentionally overflow the return value, leading to arbitrary heap writes. Because the resulting array is then passed to `execv()`, it is possible to leverage this attack to gain remote code execution on a victim machine. Note that a victim must first allow access to `git shell` as a login shell in order to be vulnerable to this attack. This problem is patched	https://github.com/git/git/security/advisories/GHSA-rjr6-wcq6-83p6	A-GIT-GIT-041122/1387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in versions 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 and users are advised to upgrade to the latest version. Disabling `git shell` access via remote logins is a viable short-term workaround. **CVE ID : CVE-2022-39260**		
Improper Link Resolution Before File Access ('Link Following')	19-Oct-2022	5.5	Git is an open source, scalable, distributed revision control system. Versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 are subject to exposure of sensitive information to a malicious actor. When performing a local clone (where the source and target of the clone are on the same volume), Git copies the contents of the source's `$GIT_DIR/objects` directory into the destination by either creating hardlinks to the source contents, or copying them (if hardlinks are disabled via `--no-hardlinks`). A malicious actor could convince a victim to clone a repository with a symbolic link pointing at sensitive information on the victim's machine. This can be done either by having the victim	https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	A-GIT-GIT-041122/1388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clone a malicious repository on the same machine, or having them clone a malicious repository embedded as a bare repository via a submodule from any source, provided they clone with the `--recurse-submodules` option. Git does not create symbolic links in the `$GIT_DIR/objects` directory. The problem has been patched in the versions published on 2022-10-18, and backported to v2.30.x. Potential workarounds: Avoid cloning untrusted repositories using the `--local` optimization when on a shared machine, either by passing the `--no-local` option to `git clone` or cloning from a URL that uses the `file://` scheme. Alternatively, avoid cloning repositories from untrusted sources with `--recurse-submodules` or run `git config --global protocol.file.allow user`. **CVE ID : CVE-2022-39253**		
Affected Version(s): From (including) 2.35.0 Up to (excluding) 2.35.5					
Out-of-bounds Write	19-Oct-2022	8.8	Git is an open source, scalable, distributed revision control system. `git shell` is a restricted login shell that can be used to implement Git's	https://github.com/git/git/security/advisories/GHSA-rjr6-wcq6-83p6	A-GIT-GIT-041122/1389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			push/pull functionality via SSH. In versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4, the function that splits the command arguments into an array improperly uses an `int` to represent the number of entries in the array, allowing a malicious actor to intentionally overflow the return value, leading to arbitrary heap writes. Because the resulting array is then passed to `execv()`, it is possible to leverage this attack to gain remote code execution on a victim machine. Note that a victim must first allow access to `git shell` as a login shell in order to be vulnerable to this attack. This problem is patched in versions 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 and users are advised to upgrade to the latest version. Disabling `git shell` access via remote logins is a viable short-term workaround. **CVE ID : CVE-2022-39260**		
Improper Link Resolution Before File	19-Oct-2022	5.5	Git is an open source, scalable, distributed revision control system. Versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5,	https://github.com/git/git/security/advisories/G	A-GIT-GIT-041122/1390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access ('Link Following')			2.34.5, 2.35.5, 2.36.3, and 2.37.4 are subject to exposure of sensitive information to a malicious actor. When performing a local clone (where the source and target of the clone are on the same volume), Git copies the contents of the source's `$GIT_DIR/objects` directory into the destination by either creating hardlinks to the source contents, or copying them (if hardlinks are disabled via `--no-hardlinks`). A malicious actor could convince a victim to clone a repository with a symbolic link pointing at sensitive information on the victim's machine. This can be done either by having the victim clone a malicious repository on the same machine, or having them clone a malicious repository embedded as a bare repository via a submodule from any source, provided they clone with the `--recurse-submodules` option. Git does not create symbolic links in the `$GIT_DIR/objects` directory. The problem has been patched in the versions published on 2022-10-18, and	HSA-3wp6-j8xr-qw85	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			backported to v2.30.x. Potential workarounds: Avoid cloning untrusted repositories using the `--local` optimization when on a shared machine, either by passing the `--no-local` option to `git clone` or cloning from a URL that uses the `file://` scheme. Alternatively, avoid cloning repositories from untrusted sources with `--recurse-submodules` or run `git config --global protocol.file.allow user`. **CVE ID : CVE-2022-39253**		
Affected Version(s): From (including) 2.36.0 Up to (excluding) 2.36.3					
Out-of-bounds Write	19-Oct-2022	8.8	Git is an open source, scalable, distributed revision control system. `git shell` is a restricted login shell that can be used to implement Git's push/pull functionality via SSH. In versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4, the function that splits the command arguments into an array improperly uses an `int` to represent the number of entries in the array, allowing a malicious actor to intentionally overflow the return value, leading to arbitrary heap writes. Because the resulting array is then passed to	https://github.com/git/git/security/advisories/GHSA-rjr6-wcq6-83p6	A-GIT-GIT-041122/1391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`execv()`, it is possible to leverage this attack to gain remote code execution on a victim machine. Note that a victim must first allow access to `git shell` as a login shell in order to be vulnerable to this attack. This problem is patched in versions 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 and users are advised to upgrade to the latest version. Disabling `git shell` access via remote logins is a viable short-term workaround. **CVE ID : CVE-2022-39260**		
Improper Link Resolution Before File Access ('Link Following')	19-Oct-2022	5.5	Git is an open source, scalable, distributed revision control system. Versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 are subject to exposure of sensitive information to a malicious actor. When performing a local clone (where the source and target of the clone are on the same volume), Git copies the contents of the source's `$GIT_DIR/objects` directory into the destination by either creating hardlinks to the source contents, or copying them (if	https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	A-GIT-GIT-041122/1392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hardlinks are disabled via `--no-hardlinks`). A malicious actor could convince a victim to clone a repository with a symbolic link pointing at sensitive information on the victim's machine. This can be done either by having the victim clone a malicious repository on the same machine, or having them clone a malicious repository embedded as a bare repository via a submodule from any source, provided they clone with the `--recurse-submodules` option. Git does not create symbolic links in the `$GIT_DIR/objects` directory. The problem has been patched in the versions published on 2022-10-18, and backported to v2.30.x. Potential workarounds: Avoid cloning untrusted repositories using the `--local` optimization when on a shared machine, either by passing the `--no-local` option to `git clone` or cloning from a URL that uses the `file://` scheme. Alternatively, avoid cloning repositories from untrusted sources with `--recurse-submodules` or run `git config --global protocol.file.allow user`.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39253		
Affected Version(s): From (including) 2.37.0 Up to (excluding) 2.37.4					
Out-of-bounds Write	19-Oct-2022	8.8	Git is an open source, scalable, distributed revision control system. `git shell` is a restricted login shell that can be used to implement Git's push/pull functionality via SSH. In versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4, the function that splits the command arguments into an array improperly uses an `int` to represent the number of entries in the array, allowing a malicious actor to intentionally overflow the return value, leading to arbitrary heap writes. Because the resulting array is then passed to `execv()`, it is possible to leverage this attack to gain remote code execution on a victim machine. Note that a victim must first allow access to `git shell` as a login shell in order to be vulnerable to this attack. This problem is patched in versions 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 and users are advised to upgrade to the latest version. Disabling `git shell` access via remote	https://github.com/git/git/security/advisories/GHSA-rjr6-wcq6-83p6	A-GIT-GIT-041122/1393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logins is a viable short-term workaround. **CVE ID : CVE-2022-39260**		
Improper Link Resolution Before File Access ('Link Following')	19-Oct-2022	5.5	Git is an open source, scalable, distributed revision control system. Versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 are subject to exposure of sensitive information to a malicious actor. When performing a local clone (where the source and target of the clone are on the same volume), Git copies the contents of the source's `$GIT_DIR/objects` directory into the destination by either creating hardlinks to the source contents, or copying them (if hardlinks are disabled via `--no-hardlinks`). A malicious actor could convince a victim to clone a repository with a symbolic link pointing at sensitive information on the victim's machine. This can be done either by having the victim clone a malicious repository on the same machine, or having them clone a malicious repository embedded as a bare repository via a submodule from any	https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	A-GIT-GIT-041122/1394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			source, provided they clone with the `--recurse-submodules` option. Git does not create symbolic links in the `$GIT_DIR/objects` directory. The problem has been patched in the versions published on 2022-10-18, and backported to v2.30.x. Potential workarounds: Avoid cloning untrusted repositories using the `--local` optimization when on a shared machine, either by passing the `--no-local` option to `git clone` or cloning from a URL that uses the `file://` scheme. Alternatively, avoid cloning repositories from untrusted sources with `--recurse-submodules` or run `git config --global protocol.file.allow user`. **CVE ID : CVE-2022-39253**		
Vendor: gitea					
Product: gitea					
Affected Version(s): * Up to (excluding) 1.17.3					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	16-Oct-2022	9.8	Gitea before 1.17.3 does not sanitize and escape refs in the git backend. Arguments to git commands are mishandled. **CVE ID : CVE-2022-42968**	https://github.com/go-gitea/gitea/pull/21463	A-GIT-GITE-041122/1395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Github					
Product: enterprise_server					
Affected Version(s): * Up to (excluding) 3.2.16					
Deserialization of Untrusted Data	19-Oct-2022	8.8	A deserialization of untrusted data vulnerability was identified in GitHub Enterprise Server that could potentially lead to remote code execution on the SVNBridge. To exploit this vulnerability, an attacker would need to gain access via a server-side request forgery (SSRF) that would let an attacker control the data being deserialized. This vulnerability affected all versions of GitHub Enterprise Server prior to v3.6 and was fixed in versions 3.5.3, 3.4.6, 3.3.11, and 3.2.16. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2022-23734**	https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.11, https://docs.github.com/en/enterprise-server@3.5/admin/release-notes#3.5.3, https://docs.github.com/en/enterprise-server@3.2/admin/release-notes#3.2.16	A-GIT-ENTE-041122/1396
Affected Version(s): From (including) 3.3.0 Up to (excluding) 3.3.11					
Deserialization of Untrusted Data	19-Oct-2022	8.8	A deserialization of untrusted data vulnerability was identified in GitHub Enterprise Server that could potentially lead to remote code execution on the SVNBridge. To exploit this vulnerability, an attacker would need to gain access via a	https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.11, https://docs.github.com/	A-GIT-ENTE-041122/1397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server-side request forgery (SSRF) that would let an attacker control the data being deserialized. This vulnerability affected all versions of GitHub Enterprise Server prior to v3.6 and was fixed in versions 3.5.3, 3.4.6, 3.3.11, and 3.2.16. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2022-23734**	en/enterprise-server@3.5/admin/release-notes#3.5.3, https://docs.github.com/en/enterprise-server@3.2/admin/release-notes#3.2.16	
Affected Version(s): From (including) 3.4.0 Up to (excluding) 3.4.6					
Deserialization of Untrusted Data	19-Oct-2022	8.8	A deserialization of untrusted data vulnerability was identified in GitHub Enterprise Server that could potentially lead to remote code execution on the SVNBridge. To exploit this vulnerability, an attacker would need to gain access via a server-side request forgery (SSRF) that would let an attacker control the data being deserialized. This vulnerability affected all versions of GitHub Enterprise Server prior to v3.6 and was fixed in versions 3.5.3, 3.4.6, 3.3.11, and 3.2.16. This vulnerability was reported via the GitHub Bug Bounty program.	https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.11, https://docs.github.com/en/enterprise-server@3.5/admin/release-notes#3.5.3, https://docs.github.com/en/enterprise-server@3.2/admin/release-notes#3.2.16	A-GIT-ENTE-041122/1398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23734		
Affected Version(s): From (including) 3.5.0 Up to (excluding) 3.5.3					
Deserialization of Untrusted Data	19-Oct-2022	8.8	A deserialization of untrusted data vulnerability was identified in GitHub Enterprise Server that could potentially lead to remote code execution on the SVNBridge. To exploit this vulnerability, an attacker would need to gain access via a server-side request forgery (SSRF) that would let an attacker control the data being deserialized. This vulnerability affected all versions of GitHub Enterprise Server prior to v3.6 and was fixed in versions 3.5.3, 3.4.6, 3.3.11, and 3.2.16. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2022-23734**	https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.11, https://docs.github.com/en/enterprise-server@3.5/admin/release-notes#3.5.3, https://docs.github.com/en/enterprise-server@3.2/admin/release-notes#3.2.16	A-GIT-ENTE-041122/1399
Product: runner					
Affected Version(s): * Up to (excluding) 2.283.4					
Improper Neutralization of Special Elements used in an OS Command ('OS	25-Oct-2022	9.9	GitHub Actions Runner is the application that runs a job from a GitHub Actions workflow. The actions runner invokes the docker cli directly in order to run job containers, service containers, or container actions. A bug in the logic	https://github.com/actions/runner/pull/2107, https://github.com/actions/runner/pull/2108, https://github.com/acti	A-GIT-RUNN-041122/1400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			for how the environment is encoded into these docker commands was discovered in versions prior to 2.296.2, 2.293.1, 2.289.4, 2.285.2, and 2.283.4 that allows an input to escape the environment variable and modify that docker command invocation directly. Jobs that use container actions, job containers, or service containers alongside untrusted user inputs in environment variables may be vulnerable. The Actions Runner has been patched, both on `github.com` and hotfixes for GHES and GHAE customers in versions 2.296.2, 2.293.1, 2.289.4, 2.285.2, and 2.283.4. GHES and GHAE customers may want to patch their instance in order to have their runners automatically upgrade to these new runner versions. As a workaround, users may consider removing any container actions, job containers, or service containers from their jobs until they are able to upgrade their runner versions. **CVE ID : CVE-2022-39321**	ons/runner/security/advisories/GHSA-2c6m-6gqh-6qg3	
Affected Version(s): From (including) 2.284.0 Up to (excluding) 2.285.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.9	GitHub Actions Runner is the application that runs a job from a GitHub Actions workflow. The actions runner invokes the docker cli directly in order to run job containers, service containers, or container actions. A bug in the logic for how the environment is encoded into these docker commands was discovered in versions prior to 2.296.2, 2.293.1, 2.289.4, 2.285.2, and 2.283.4 that allows an input to escape the environment variable and modify that docker command invocation directly. Jobs that use container actions, job containers, or service containers alongside untrusted user inputs in environment variables may be vulnerable. The Actions Runner has been patched, both on `github.com` and hotfixes for GHES and GHAE customers in versions 2.296.2, 2.293.1, 2.289.4, 2.285.2, and 2.283.4. GHES and GHAE customers may want to patch their instance in order to have their runners automatically upgrade to these new runner versions. As a workaround, users may consider removing any	https://github.com/actions/runner/pull/2107, https://github.com/actions/runner/pull/2108, https://github.com/actions/runner/security/advisories/GHSA-2c6m-6gqh-6qg3	A-GIT-RUNN-041122/1401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			container actions, job containers, or service containers from their jobs until they are able to upgrade their runner versions. **CVE ID : CVE-2022-39321**		
Affected Version(s): From (including) 2.286.0 Up to (excluding) 2.289.4					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.9	GitHub Actions Runner is the application that runs a job from a GitHub Actions workflow. The actions runner invokes the docker cli directly in order to run job containers, service containers, or container actions. A bug in the logic for how the environment is encoded into these docker commands was discovered in versions prior to 2.296.2, 2.293.1, 2.289.4, 2.285.2, and 2.283.4 that allows an input to escape the environment variable and modify that docker command invocation directly. Jobs that use container actions, job containers, or service containers alongside untrusted user inputs in environment variables may be vulnerable. The Actions Runner has been patched, both on `github.com` and hotfixes for GHES and GHAE customers in versions 2.296.2, 2.293.1, 2.289.4,	https://github.com/actions/runner/pull/2107, https://github.com/actions/runner/pull/2108, https://github.com/actions/runner/security/advisories/GHSA-2c6m-6gqh-6qg3	A-GIT-RUNN-041122/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.285.2, and 2.283.4. GHES and GHAE customers may want to patch their instance in order to have their runners automatically upgrade to these new runner versions. As a workaround, users may consider removing any container actions, job containers, or service containers from their jobs until they are able to upgrade their runner versions. **CVE ID : CVE-2022-39321**		
Affected Version(s): From (including) 2.290.0 Up to (excluding) 2.293.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.9	GitHub Actions Runner is the application that runs a job from a GitHub Actions workflow. The actions runner invokes the docker cli directly in order to run job containers, service containers, or container actions. A bug in the logic for how the environment is encoded into these docker commands was discovered in versions prior to 2.296.2, 2.293.1, 2.289.4, 2.285.2, and 2.283.4 that allows an input to escape the environment variable and modify that docker command invocation directly. Jobs that use container actions, job containers, or service	https://github.com/actions/runner/pull/2107, https://github.com/actions/runner/pull/2108, https://github.com/actions/runner/security/advisories/GHSA-2c6m-6gqh-6qg3	A-GIT-RUNN-041122/1403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containers alongside untrusted user inputs in environment variables may be vulnerable. The Actions Runner has been patched, both on `github.com` and hotfixes for GHES and GHAE customers in versions 2.296.2, 2.293.1, 2.289.4, 2.285.2, and 2.283.4. GHES and GHAE customers may want to patch their instance in order to have their runners automatically upgrade to these new runner versions. As a workaround, users may consider removing any container actions, job containers, or service containers from their jobs until they are able to upgrade their runner versions. **CVE ID : CVE-2022-39321**		
Affected Version(s): From (including) 2.294.0 Up to (excluding) 2.296.2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.9	GitHub Actions Runner is the application that runs a job from a GitHub Actions workflow. The actions runner invokes the docker cli directly in order to run job containers, service containers, or container actions. A bug in the logic for how the environment is encoded into these docker commands was discovered in versions	https://github.com/actions/runner/pull/2107, https://github.com/actions/runner/pull/2108, https://github.com/actions/runner/security/advisories/GHS	A-GIT-RUNN-041122/1404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 2.296.2, 2.293.1, 2.289.4, 2.285.2, and 2.283.4 that allows an input to escape the environment variable and modify that docker command invocation directly. Jobs that use container actions, job containers, or service containers alongside untrusted user inputs in environment variables may be vulnerable. The Actions Runner has been patched, both on `github.com` and hotfixes for GHES and GHAE customers in versions 2.296.2, 2.293.1, 2.289.4, 2.285.2, and 2.283.4. GHES and GHAE customers may want to patch their instance in order to have their runners automatically upgrade to these new runner versions. As a workaround, users may consider removing any container actions, job containers, or service containers from their jobs until they are able to upgrade their runner versions. **CVE ID : CVE-2022-39321**	A-2c6m-6gqh-6qg3	
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): * Up to (excluding) 15.1.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	17-Oct-2022	7.5	A potential DOS vulnerability was discovered in GitLab CE/EE affecting all versions before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. Malformed content added to the issue description could have been used to trigger high CPU usage. **CVE ID : CVE-2022-2931**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2931.json	A-GIT-GITL-041122/1405
N/A	17-Oct-2022	7.5	An issue has been discovered in GitLab CE/EE affecting all versions before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. It may be possible for an attacker to guess a user's password by brute force by sending crafted requests to a specific endpoint, even if the victim user has 2FA enabled on their account. **CVE ID : CVE-2022-3031**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3031.json	A-GIT-GITL-041122/1406
Improper Neutralization of Input During Web Page Generation ('Cross-site	17-Oct-2022	7.3	A crafted tag in the Jupyter Notebook viewer in GitLab EE/CE affecting all versions before 15.1.6, 15.2 to 15.2.4, and 15.3 to 15.3.2 allows an attacker to issue arbitrary HTTP requests	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2428.json	A-GIT-GITL-041122/1407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			**CVE ID : CVE-2022-2428**		
Improper Input Validation	17-Oct-2022	6.5	A lack of length validation in Snippet descriptions in GitLab CE/EE affecting all versions prior to 15.1.6, 15.2 prior to 15.2.4 and 15.3 prior to 15.3.2 allows an authenticated attacker to create a maliciously large Snippet which when requested with or without authentication places excessive load on the server, potential leading to Denial of Service. **CVE ID : CVE-2022-2592**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2592.json	A-GIT-GITL-041122/1408
N/A	17-Oct-2022	4.3	An improper access control issue in GitLab CE/EE affecting all versions starting before 15.1.6, all versions from 15.2 before 15.2.4, all versions from 15.3 before 15.3.2 allows disclosure of pipeline status to unauthorized users. **CVE ID : CVE-2022-3030**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3030.json	A-GIT-GITL-041122/1409
Affected Version(s): * Up to (excluding) 15.2.5					
Uncontrolled Resource Consumption	17-Oct-2022	7.5	A potential DOS vulnerability was discovered in GitLab CE/EE affecting all versions before before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions	https://gitlab.com/gitlab-org/gitlab/-/issues/361982, https://gitlab.com/gitlab-org/cves/-	A-GIT-GITL-041122/1410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			starting from 15.4 before 15.4.1 While cloning an issue with special crafted content added to the description could have been used to trigger high CPU usage. **CVE ID : CVE-2022-3283**	/blob/master/2022/CVE-2022-3283.json	
Improper Handling of Exceptional Conditions	17-Oct-2022	6.5	An unhandled exception in job log parsing in GitLab CE/EE affecting all versions prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows an attacker to prevent access to job logs **CVE ID : CVE-2022-3279**	https://gitlab.com/gitlab-org/gitlab/-/issues/364249, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3279.json	A-GIT-GITL-041122/1411
N/A	17-Oct-2022	4.3	A branch/tag name confusion in GitLab CE/EE affecting all versions prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows an attacker to manipulate pages where the content of the default branch would be expected. **CVE ID : CVE-2022-3288**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3288.json, https://gitlab.com/gitlab-org/gitlab/-/issues/354948	A-GIT-GITL-041122/1412
Affected Version(s): * Up to (including) 12.7.0					
Improper Neutralization of Special Elements in Output Used by a	17-Oct-2022	7.3	Improper control of a resource identifier in Error Tracking in GitLab CE/EE affecting all versions from 12.7 allows an authenticated attacker to generate	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3060.json	A-GIT-GITL-041122/1413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Downstream Component ('Injection')			content which could cause a victim to make unintended arbitrary requests **CVE ID : CVE-2022-3060**		
Affected Version(s): From (including) 10.0.0 Up to (excluding) 15.1.6					
Uncontrolled Resource Consumption	17-Oct-2022	6.5	A business logic issue in the handling of large repositories in all versions of GitLab CE/EE from 10.0 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2 allowed an authenticated and authorized user to exhaust server resources by importing a malicious project. **CVE ID : CVE-2022-2455**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2455.json	A-GIT-GITL-041122/1414
Affected Version(s): From (including) 10.0.0 Up to (excluding) 15.2.5					
N/A	17-Oct-2022	5.4	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. It was possible for an unauthorised user to create issues in a project. **CVE ID : CVE-2022-3066**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3066.json	A-GIT-GITL-041122/1415
Affected Version(s): From (including) 10.7.0 Up to (excluding) 15.1.5					
Uncontrolled Resource	17-Oct-2022	4.3	A potential DoS vulnerability was discovered in Gitlab	https://gitlab.com/gitlab-org/cves/-	A-GIT-GITL-041122/1416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			CE/EE versions starting from 10.7 before 15.1.5, all versions starting from 15.2 before 15.2.3, all versions starting from 15.3 before 15.3.1 allowed an attacker to trigger high CPU usage via a special crafted input added in the Commit message field. **CVE ID : CVE-2022-2908**	/blob/master/2022/CVE-2022-2908.json	
Affected Version(s): From (including) 10.8.0 Up to (excluding) 15.1.6					
Uncontrolled Resource Consumption	21-Oct-2022	7.5	A potential DOS vulnerability was discovered in GitLab CE/EE affecting all versions from 10.8 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. Improper data handling on branch creation could have been used to trigger high CPU usage. **CVE ID : CVE-2022-3639**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3639.json	A-GIT-GITL-041122/1417
Affected Version(s): From (including) 11.10 Up to (excluding) 15.1.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Oct-2022	9.9	A vulnerability in GitLab CE/EE affecting all versions from 11.10 prior to 15.1.6, 15.2 to 15.2.4, 15.3 to 15.3.2 allows an authenticated user to achieve remote code execution via the Import from GitHub API endpoint.	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2992.json	A-GIT-GITL-041122/1418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2992		
Affected Version(s): From (including) 11.3.4 Up to (excluding) 15.1.5					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Oct-2022	9.9	A vulnerability in GitLab CE/EE affecting all versions from 11.3.4 prior to 15.1.5, 15.2 to 15.2.3, 15.3 to 15.3 to 15.3.1 allows an an authenticated user to achieve remote code execution via the Import from GitHub API endpoint **CVE ID : CVE-2022-2884**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2884.json	A-GIT-GITL-041122/1419
Affected Version(s): From (including) 12.10 Up to (excluding) 15.1.6					
Improper Authentication	17-Oct-2022	7.4	An issue has been discovered in GitLab affecting all versions starting from 12.10 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. GitLab was not performing correct authentication with some Package Registries when IP address restrictions were configured, allowing an attacker already in possession of a valid Deploy Token to misuse it from any location. **CVE ID : CVE-2022-2533**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2533.json	A-GIT-GITL-041122/1420
Affected Version(s): From (including) 12.6.0 Up to (excluding) 15.2.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	28-Oct-2022	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.6 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. A malicious maintainer could exfiltrate a GitHub integration's access token by modifying the integration URL such that authenticated requests are sent to an attacker controlled server. **CVE ID : CVE-2022-2882**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2882.json	A-GIT-GITL-041122/1421
Affected Version(s): From (including) 12.8.0 Up to (excluding) 15.2.5					
Incorrect Permission Assignment for Critical Resource	17-Oct-2022	4.3	Improper access control in the GitLab CE/EE API affecting all versions starting from 12.8 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. Allowed for editing the approval rules via the API by an unauthorised user. **CVE ID : CVE-2022-3325**	https://gitlab.com/gitlab-org/gitlab/-/issues/360819, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3325.json	A-GIT-GITL-041122/1422
Affected Version(s): From (including) 13.7.0 Up to (excluding) 15.2.5					
Exposure of Sensitive Information to an	17-Oct-2022	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 13.7 before 15.2.5, all versions starting from 15.3 before	https://gitlab.com/gitlab-org/gitlab/-/issues/364266, https://gitla	A-GIT-GITL-041122/1423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			15.3.4, all versions starting from 15.4 before 15.4.1. A user's primary email may be disclosed to an attacker through group member events webhooks. **CVE ID : CVE-2022-3351**	b.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3351.json	
Affected Version(s): From (including) 14.2 Up to (excluding) 15.2.5					
N/A	17-Oct-2022	5.3	Lack of IP address checking in GitLab EE affecting all versions from 14.2 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows a group member to bypass IP restrictions when using a deploy token **CVE ID : CVE-2022-3286**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3286.json, https://gitlab.com/gitlab-org/gitlab/-/issues/363827	A-GIT-GITL-041122/1424
Affected Version(s): From (including) 14.4 Up to (excluding) 15.2.5					
N/A	17-Oct-2022	6.5	An issue has been discovered in the Import functionality of GitLab CE/EE affecting all versions starting from 14.4 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. It was possible for an authenticated user to read arbitrary projects' content given the project's ID. **CVE ID : CVE-2022-3067**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3067.json	A-GIT-GITL-041122/1425
Affected Version(s): From (including) 14.5 Up to (excluding) 15.1.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorization Bypass Through User-Controlled Key	17-Oct-2022	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 14.5 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. GitLab's Zentao integration has an insecure direct object reference vulnerability that may be exploited by an attacker to leak Zentao project issues. **CVE ID : CVE-2022-3331**	https://gitlab.com/gitlab-org/gitlab/-/issues/360372, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3331.json	A-GIT-GITL-041122/1426
Affected Version(s): From (including) 14.9 Up to (excluding) 15.2.5					
Deserialization of Untrusted Data	17-Oct-2022	6.5	Serialization of sensitive data in GitLab EE affecting all versions from 14.9 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 can leak sensitive information via cache **CVE ID : CVE-2022-3291**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3291.json, https://gitlab.com/gitlab-org/gitlab/-/issues/354299	A-GIT-GITL-041122/1427
Affected Version(s): From (including) 14.9.0 Up to (excluding) 15.1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	8	An issue in Incident Timelines has been discovered in GitLab CE/EE affecting all versions starting from 14.9 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2.which allowed an authenticated	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2527.json	A-GIT-GITL-041122/1428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to inject arbitrary content. A victim interacting with this content could lead to arbitrary requests. **CVE ID : CVE-2022-2527**		
Affected Version(s): From (including) 15.0.0 Up to (excluding) 15.2.5					
Incorrect Authorization	17-Oct-2022	4.3	It was possible for a guest user to read a todo targeting an inaccessible note in Gitlab CE/EE affecting all versions from 15.0 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1. **CVE ID : CVE-2022-3330**	https://gitlab.com/gitlab-org/gitlab/-/issues/365827, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3330.json	A-GIT-GITL-041122/1429
Affected Version(s): From (including) 15.2 Up to (excluding) 15.2.3					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Oct-2022	9.9	A vulnerability in GitLab CE/EE affecting all versions from 11.3.4 prior to 15.1.5, 15.2 to 15.2.3, 15.3 to 15.3 to 15.3.1 allows an an authenticated user to achieve remote code execution via the Import from GitHub API endpoint **CVE ID : CVE-2022-2884**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2884.json	A-GIT-GITL-041122/1430
Uncontrolled Resource Consumption	17-Oct-2022	4.3	A potential DoS vulnerability was discovered in Gitlab CE/EE versions starting from 10.7 before 15.1.5, all versions starting from 15.2 before 15.2.3, all versions starting from	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2908.json	A-GIT-GITL-041122/1431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.3 before 15.3.1 allowed an attacker to trigger high CPU usage via a special crafted input added in the Commit message field. **CVE ID : CVE-2022-2908**		
Affected Version(s): From (including) 15.2 Up to (excluding) 15.2.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Oct-2022	9.9	A vulnerability in GitLab CE/EE affecting all versions from 11.10 prior to 15.1.6, 15.2 to 15.2.4, 15.3 to 15.3.2 allows an authenticated user to achieve remote code execution via the Import from GitHub API endpoint. **CVE ID : CVE-2022-2992**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2992.json	A-GIT-GITL-041122/1432
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	8	An issue in Incident Timelines has been discovered in GitLab CE/EE affecting all versions starting from 14.9 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2.which allowed an authenticated attacker to inject arbitrary content. A victim interacting with this content could lead to arbitrary requests. **CVE ID : CVE-2022-2527**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2527.json	A-GIT-GITL-041122/1433
Uncontrolled Resource	17-Oct-2022	7.5	A potential DOS vulnerability was discovered in GitLab	https://gitlab.com/gitlab-org/cves/-	A-GIT-GITL-041122/1434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			CE/EE affecting all versions before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. Malformed content added to the issue description could have been used to trigger high CPU usage. **CVE ID : CVE-2022-2931**	/blob/master/2022/CVE-2022-2931.json	
N/A	17-Oct-2022	7.5	An issue has been discovered in GitLab CE/EE affecting all versions before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. It may be possible for an attacker to guess a user's password by brute force by sending crafted requests to a specific endpoint, even if the victim user has 2FA enabled on their account. **CVE ID : CVE-2022-3031**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3031.json	A-GIT-GITL-041122/1435
Uncontrolled Resource Consumption	21-Oct-2022	7.5	A potential DOS vulnerability was discovered in GitLab CE/EE affecting all versions from 10.8 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. Improper data handling on branch creation could	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3639.json	A-GIT-GITL-041122/1436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have been used to trigger high CPU usage. **CVE ID : CVE-2022-3639**		
Improper Authentication	17-Oct-2022	7.4	An issue has been discovered in GitLab affecting all versions starting from 12.10 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. GitLab was not performing correct authentication with some Package Registries when IP address restrictions were configured, allowing an attacker already in possession of a valid Deploy Token to misuse it from any location. **CVE ID : CVE-2022-2533**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2533.json	A-GIT-GITL-041122/1437
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	7.3	A crafted tag in the Jupyter Notebook viewer in GitLab EE/CE affecting all versions before 15.1.6, 15.2 to 15.2.4, and 15.3 to 15.3.2 allows an attacker to issue arbitrary HTTP requests **CVE ID : CVE-2022-2428**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2428.json	A-GIT-GITL-041122/1438
Uncontrolled Resource Consumption	17-Oct-2022	6.5	A business logic issue in the handling of large repositories in all versions of GitLab CE/EE from 10.0 before 15.1.6,	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE	A-GIT-GITL-041122/1439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2 allowed an authenticated and authorized user to exhaust server resources by importing a malicious project. **CVE ID : CVE-2022-2455**	-2022-2455.json	
Improper Input Validation	17-Oct-2022	6.5	A lack of length validation in Snippet descriptions in GitLab CE/EE affecting all versions prior to 15.1.6, 15.2 prior to 15.2.4 and 15.3 prior to 15.3.2 allows an authenticated attacker to create a maliciously large Snippet which when requested with or without authentication places excessive load on the server, potential leading to Denial of Service. **CVE ID : CVE-2022-2592**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2592.json	A-GIT-GITL-041122/1440
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	4.8	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions before 15.1.6, 15.2 to 15.2.4 and 15.3 prior to 15.3.2. It was possible to exploit a vulnerability in setting the labels colour feature which could lead to a stored XSS that allowed attackers to perform arbitrary actions on	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2865.json	A-GIT-GITL-041122/1441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behalf of victims at client side. **CVE ID : CVE-2022-2865**		
N/A	17-Oct-2022	4.3	An improper access control issue in GitLab CE/EE affecting all versions starting from 15.2 before 15.2.4, all versions from 15.3 before 15.3.2 allows disclosure of confidential information via the Incident timeline events. **CVE ID : CVE-2022-2630**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2630.json	A-GIT-GITL-041122/1442
N/A	17-Oct-2022	4.3	An improper access control issue in GitLab CE/EE affecting all versions starting before 15.1.6, all versions from 15.2 before 15.2.4, all versions from 15.3 before 15.3.2 allows disclosure of pipeline status to unauthorized users. **CVE ID : CVE-2022-3030**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3030.json	A-GIT-GITL-041122/1443
Authorization Bypass Through User-Controlled Key	17-Oct-2022	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 14.5 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. GitLab's Zentao integration has an insecure direct object reference vulnerability that may be exploited by	https://gitlab.com/gitlab-org/gitlab/-/issues/360372, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3331.json	A-GIT-GITL-041122/1444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an attacker to leak Zentao project issues. **CVE ID : CVE-2022-3331**		
Affected Version(s): From (including) 15.3 Up to (excluding) 15.3.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Oct-2022	9.9	A vulnerability in GitLab CE/EE affecting all versions from 11.3.4 prior to 15.1.5, 15.2 to 15.2.3, 15.3 to 15.3 to 15.3.1 allows an an authenticated user to achieve remote code execution via the Import from GitHub API endpoint **CVE ID : CVE-2022-2884**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2884.json	A-GIT-GITL-041122/1445
Uncontrolled Resource Consumption	17-Oct-2022	4.3	A potential DoS vulnerability was discovered in Gitlab CE/EE versions starting from 10.7 before 15.1.5, all versions starting from 15.2 before 15.2.3, all versions starting from 15.3 before 15.3.1 allowed an attacker to trigger high CPU usage via a special crafted input added in the Commit message field. **CVE ID : CVE-2022-2908**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2908.json	A-GIT-GITL-041122/1446
Affected Version(s): From (including) 15.3 Up to (excluding) 15.3.2					
Improper Neutralization of Special Elements used in a	17-Oct-2022	9.9	A vulnerability in GitLab CE/EE affecting all versions from 11.10 prior to 15.1.6, 15.2 to 15.2.4, 15.3 to 15.3.2 allows an authenticated	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE	A-GIT-GITL-041122/1447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			user to achieve remote code execution via the Import from GitHub API endpoint. **CVE ID : CVE-2022-2992**	-2022-2992.json	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	8	An issue in Incident Timelines has been discovered in GitLab CE/EE affecting all versions starting from 14.9 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2.which allowed an authenticated attacker to inject arbitrary content. A victim interacting with this content could lead to arbitrary requests. **CVE ID : CVE-2022-2527**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2527.json	A-GIT-GITL-041122/1448
Uncontrolled Resource Consumption	17-Oct-2022	7.5	A potential DOS vulnerability was discovered in GitLab CE/EE affecting all versions before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. Malformed content added to the issue description could have been used to trigger high CPU usage. **CVE ID : CVE-2022-2931**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2931.json	A-GIT-GITL-041122/1449
N/A	17-Oct-2022	7.5	An issue has been discovered in GitLab	https://gitlab.com/gitlab	A-GIT-GITL-041122/1450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CE/EE affecting all versions before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. It may be possible for an attacker to guess a user's password by brute force by sending crafted requests to a specific endpoint, even if the victim user has 2FA enabled on their account. **CVE ID : CVE-2022-3031**	-org/cves/-/blob/master/2022/CVE-2022-3031.json	
Uncontrolled Resource Consumption	21-Oct-2022	7.5	A potential DOS vulnerability was discovered in GitLab CE/EE affecting all versions from 10.8 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. Improper data handling on branch creation could have been used to trigger high CPU usage. **CVE ID : CVE-2022-3639**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3639.json	A-GIT-GITL-041122/1451
Improper Authentication	17-Oct-2022	7.4	An issue has been discovered in GitLab affecting all versions starting from 12.10 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. GitLab was not performing correct	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2533.json	A-GIT-GITL-041122/1452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication with some Package Registries when IP address restrictions were configured, allowing an attacker already in possession of a valid Deploy Token to misuse it from any location. **CVE ID : CVE-2022-2533**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	7.3	A crafted tag in the Jupyter Notebook viewer in GitLab EE/CE affecting all versions before 15.1.6, 15.2 to 15.2.4, and 15.3 to 15.3.2 allows an attacker to issue arbitrary HTTP requests **CVE ID : CVE-2022-2428**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2428.json	A-GIT-GITL-041122/1453
Uncontrolled Resource Consumption	17-Oct-2022	6.5	A business logic issue in the handling of large repositories in all versions of GitLab CE/EE from 10.0 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2 allowed an authenticated and authorized user to exhaust server resources by importing a malicious project. **CVE ID : CVE-2022-2455**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2455.json	A-GIT-GITL-041122/1454
Improper Input Validation	17-Oct-2022	6.5	A lack of length validation in Snippet descriptions in GitLab CE/EE affecting all	https://gitlab.com/gitlab-org/cves/-/blob/maste	A-GIT-GITL-041122/1455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 15.1.6, 15.2 prior to 15.2.4 and 15.3 prior to 15.3.2 allows an authenticated attacker to create a maliciously large Snippet which when requested with or without authentication places excessive load on the server, potential leading to Denial of Service. **CVE ID : CVE-2022-2592**	r/2022/CVE-2022-2592.json	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	4.8	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions before 15.1.6, 15.2 to 15.2.4 and 15.3 prior to 15.3.2. It was possible to exploit a vulnerability in setting the labels colour feature which could lead to a stored XSS that allowed attackers to perform arbitrary actions on behalf of victims at client side. **CVE ID : CVE-2022-2865**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2865.json	A-GIT-GITL-041122/1456
N/A	17-Oct-2022	4.3	An improper access control issue in GitLab CE/EE affecting all versions starting from 15.2 before 15.2.4, all versions from 15.3 before 15.3.2 allows disclosure of confidential information via the Incident timeline events.	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2630.json	A-GIT-GITL-041122/1457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2630		
N/A	17-Oct-2022	4.3	An improper access control issue in GitLab CE/EE affecting all versions starting before 15.1.6, all versions from 15.2 before 15.2.4, all versions from 15.3 before 15.3.2 allows disclosure of pipeline status to unauthorized users. **CVE ID : CVE-2022-3030**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3030.json	A-GIT-GITL-041122/1458
Authorization Bypass Through User-Controlled Key	17-Oct-2022	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 14.5 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. GitLab's Zentao integration has an insecure direct object reference vulnerability that may be exploited by an attacker to leak Zentao project issues. **CVE ID : CVE-2022-3331**	https://gitlab.com/gitlab-org/gitlab/-/issues/360372, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3331.json	A-GIT-GITL-041122/1459
Affected Version(s): From (including) 15.3 Up to (excluding) 15.3.4					
Uncontrolled Resource Consumption	17-Oct-2022	7.5	A potential DOS vulnerability was discovered in GitLab CE/EE affecting all versions before before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before	https://gitlab.com/gitlab-org/gitlab/-/issues/361982, https://gitlab.com/gitlab-org/cves/-/blob/maste	A-GIT-GITL-041122/1460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.4.1 While cloning an issue with special crafted content added to the description could have been used to trigger high CPU usage. **CVE ID : CVE-2022-3283**	r/2022/CVE-2022-3283.json	
N/A	17-Oct-2022	6.5	An issue has been discovered in the Import functionality of GitLab CE/EE affecting all versions starting from 14.4 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. It was possible for an authenticated user to read arbitrary projects' content given the project's ID. **CVE ID : CVE-2022-3067**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3067.json	A-GIT-GITL-041122/1461
Improper Handling of Exceptional Conditions	17-Oct-2022	6.5	An unhandled exception in job log parsing in GitLab CE/EE affecting all versions prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows an attacker to prevent access to job logs **CVE ID : CVE-2022-3279**	https://gitlab.com/gitlab-org/gitlab/-/issues/364249, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3279.json	A-GIT-GITL-041122/1462
Deserialization of Untrusted Data	17-Oct-2022	6.5	Serialization of sensitive data in GitLab EE affecting all versions from 14.9 prior to 15.2.5, 15.3 prior to 15.3.4, and	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE	A-GIT-GITL-041122/1463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.4 prior to 15.4.1 can leak sensitive information via cache **CVE ID : CVE-2022-3291**	-2022-3291.json, https://gitlab.com/gitlab-org/gitlab/-/issues/354299	
N/A	17-Oct-2022	5.4	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. It was possible for an unauthorised user to create issues in a project. **CVE ID : CVE-2022-3066**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3066.json	A-GIT-GITL-041122/1464
N/A	17-Oct-2022	5.3	Lack of IP address checking in GitLab EE affecting all versions from 14.2 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows a group member to bypass IP restrictions when using a deploy token **CVE ID : CVE-2022-3286**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3286.json, https://gitlab.com/gitlab-org/gitlab/-/issues/363827	A-GIT-GITL-041122/1465
Exposure of Resource to Wrong Sphere	28-Oct-2022	4.9	An information disclosure vulnerability in GitLab CE/EE affecting all versions starting from 9.3 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1 allows a project maintainer to	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3018.json	A-GIT-GITL-041122/1466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access the DataDog integration API key from webhook logs. **CVE ID : CVE-2022-3018**		
Exposure of Resource to Wrong Sphere	28-Oct-2022	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.6 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. A malicious maintainer could exfiltrate a GitHub integration's access token by modifying the integration URL such that authenticated requests are sent to an attacker controlled server. **CVE ID : CVE-2022-2882**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2882.json	A-GIT-GITL-041122/1467
N/A	17-Oct-2022	4.3	A branch/tag name confusion in GitLab CE/EE affecting all versions prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows an attacker to manipulate pages where the content of the default branch would be expected. **CVE ID : CVE-2022-3288**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3288.json, https://gitlab.com/gitlab-org/gitlab/-/issues/354948	A-GIT-GITL-041122/1468
Insertion of Sensitive Informati	17-Oct-2022	4.3	Email addresses were leaked in WebHook logs in GitLab EE affecting all versions from 9.3 prior	https://gitlab.com/gitlab-org/gitlab/-/issues/369	A-GIT-GITL-041122/1469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on into Log File			to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 **CVE ID : CVE-2022-3293**	008, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3293.json	
Incorrect Permission Assignment for Critical Resource	17-Oct-2022	4.3	Improper access control in the GitLab CE/EE API affecting all versions starting from 12.8 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. Allowed for editing the approval rules via the API by an unauthorised user. **CVE ID : CVE-2022-3325**	https://gitlab.com/gitlab-org/gitlab/-/issues/360819, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3325.json	A-GIT-GITL-041122/1470
Incorrect Authorization	17-Oct-2022	4.3	It was possible for a guest user to read a todo targeting an inaccessible note in Gitlab CE/EE affecting all versions from 15.0 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1. **CVE ID : CVE-2022-3330**	https://gitlab.com/gitlab-org/gitlab/-/issues/365827, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3330.json	A-GIT-GITL-041122/1471
Exposure of Sensitive Information to an Unauthorized Actor	17-Oct-2022	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 13.7 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. A user's primary	https://gitlab.com/gitlab-org/gitlab/-/issues/364266, https://gitlab.com/gitlab-org/cves/-/blob/maste	A-GIT-GITL-041122/1472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			email may be disclosed to an attacker through group member events webhooks. **CVE ID : CVE-2022-3351**	r/2022/CVE-2022-3351.json	
Affected Version(s): From (including) 15.4 Up to (excluding) 15.4.1					
Uncontrolled Resource Consumption	17-Oct-2022	7.5	A potential DOS vulnerability was discovered in GitLab CE/EE affecting all versions before before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1 While cloning an issue with special crafted content added to the description could have been used to trigger high CPU usage. **CVE ID : CVE-2022-3283**	https://gitlab.com/gitlab-org/gitlab/-/issues/361982, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3283.json	A-GIT-GITL-041122/1473
N/A	17-Oct-2022	6.5	An issue has been discovered in the Import functionality of GitLab CE/EE affecting all versions starting from 14.4 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. It was possible for an authenticated user to read arbitrary projects' content given the project's ID. **CVE ID : CVE-2022-3067**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3067.json	A-GIT-GITL-041122/1474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	17-Oct-2022	6.5	An unhandled exception in job log parsing in GitLab CE/EE affecting all versions prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows an attacker to prevent access to job logs **CVE ID : CVE-2022-3279**	https://gitlab.com/gitlab-org/gitlab/-/issues/364249, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3279.json	A-GIT-GITL-041122/1475
Deserialization of Untrusted Data	17-Oct-2022	6.5	Serialization of sensitive data in GitLab EE affecting all versions from 14.9 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 can leak sensitive information via cache **CVE ID : CVE-2022-3291**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3291.json, https://gitlab.com/gitlab-org/gitlab/-/issues/354299	A-GIT-GITL-041122/1476
N/A	17-Oct-2022	5.4	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. It was possible for an unauthorised user to create issues in a project. **CVE ID : CVE-2022-3066**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3066.json	A-GIT-GITL-041122/1477
N/A	17-Oct-2022	5.3	Lack of IP address checking in GitLab EE affecting all versions from 14.2 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-	A-GIT-GITL-041122/1478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a group member to bypass IP restrictions when using a deploy token **CVE ID : CVE-2022-3286**	3286.json, https://gitlab.com/gitlab-org/gitlab/-/issues/363827	
Exposure of Resource to Wrong Sphere	28-Oct-2022	4.9	An information disclosure vulnerability in GitLab CE/EE affecting all versions starting from 9.3 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1 allows a project maintainer to access the DataDog integration API key from webhook logs. **CVE ID : CVE-2022-3018**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3018.json	A-GIT-GITL-041122/1479
Exposure of Resource to Wrong Sphere	28-Oct-2022	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.6 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. A malicious maintainer could exfiltrate a GitHub integration's access token by modifying the integration URL such that authenticated requests are sent to an attacker controlled server. **CVE ID : CVE-2022-2882**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2882.json	A-GIT-GITL-041122/1480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Oct-2022	4.3	A branch/tag name confusion in GitLab CE/EE affecting all versions prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows an attacker to manipulate pages where the content of the default branch would be expected. **CVE ID : CVE-2022-3288**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3288.json, https://gitlab.com/gitlab-org/gitlab/-/issues/354948	A-GIT-GITL-041122/1481
Insertion of Sensitive Information into Log File	17-Oct-2022	4.3	Email addresses were leaked in WebHook logs in GitLab EE affecting all versions from 9.3 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 **CVE ID : CVE-2022-3293**	https://gitlab.com/gitlab-org/gitlab/-/issues/369008, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3293.json	A-GIT-GITL-041122/1482
Incorrect Permission Assignment for Critical Resource	17-Oct-2022	4.3	Improper access control in the GitLab CE/EE API affecting all versions starting from 12.8 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. Allowed for editing the approval rules via the API by an unauthorised user. **CVE ID : CVE-2022-3325**	https://gitlab.com/gitlab-org/gitlab/-/issues/360819, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3325.json	A-GIT-GITL-041122/1483
Incorrect Authorization	17-Oct-2022	4.3	It was possible for a guest user to read a todo targeting an inaccessible	https://gitlab.com/gitlab-org/gitlab/-	A-GIT-GITL-041122/1484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			note in Gitlab CE/EE affecting all versions from 15.0 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1. **CVE ID : CVE-2022-3330**	/issues/365827, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3330.json	
Exposure of Sensitive Information to an Unauthorized Actor	17-Oct-2022	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 13.7 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1. A user's primary email may be disclosed to an attacker through group member events webhooks. **CVE ID : CVE-2022-3351**	https://gitlab.com/gitlab-org/gitlab/-/issues/364266, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3351.json	A-GIT-GITL-041122/1485
Affected Version(s): From (including) 9.0.0 Up to (excluding) 15.1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	4.8	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions before 15.1.6, 15.2 to 15.2.4 and 15.3 prior to 15.3.2. It was possible to exploit a vulnerability in setting the labels colour feature which could lead to a stored XSS that allowed attackers to perform arbitrary actions on behalf of victims at client side.	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2865.json	A-GIT-GITL-041122/1486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2865		
Affected Version(s): From (including) 9.3 Up to (excluding) 15.2.5					
Insertion of Sensitive Information into Log File	17-Oct-2022	4.3	Email addresses were leaked in WebHook logs in GitLab EE affecting all versions from 9.3 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 **CVE ID : CVE-2022-3293**	https://gitlab.com/gitlab-org/gitlab/-/issues/369008, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3293.json	A-GIT-GITL-041122/1487
Affected Version(s): From (including) 9.3.0 Up to (excluding) 15.2.5					
Exposure of Resource to Wrong Sphere	28-Oct-2022	4.9	An information disclosure vulnerability in GitLab CE/EE affecting all versions starting from 9.3 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1 allows a project maintainer to access the DataDog integration API key from webhook logs. **CVE ID : CVE-2022-3018**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3018.json	A-GIT-GITL-041122/1488
Vendor: gl-inet					
Product: goodcloud					
Affected Version(s): 1.00.220412.00					
Improper Limitation of a Pathname to a Restricted Directory	27-Oct-2022	6.5	Multiple command injection vulnerabilities in GL.iNet GoodCloud IoT Device Management System Version 1.00.220412.00 via the ping and traceroute tools	N/A	A-GL--GOOD-041122/1489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			allow attackers to read arbitrary files on the system. **CVE ID : CVE-2022-42055**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2022	5.4	Multiple stored cross-site scripting (XSS) vulnerabilities in GL.iNet GoodCloud IoT Device Management System Version 1.00.220412.00 allow attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Company Name and Description text fields. **CVE ID : CVE-2022-42054**	N/A	A-GL--GOOD-041122/1490
Vendor: GNU					
Product: libtasn1					
Affected Version(s): * Up to (excluding) 4.19.0					
Out-of-bounds Read	24-Oct-2022	9.1	GNU Libtasn1 before 4.19.0 has an ETYPE_OK off-by-one array size check that affects asn1_encode_simple_der. **CVE ID : CVE-2021-46848**	https://bugs.gentoo.org/866237, https://gitlab.com/gnutls/libtasn1/-/commit/44a700d2051a666235748970c2df047ff207aeb5	A-GNU-LIBT-041122/1491
Vendor: go-admin					
Product: go-admin					
Affected Version(s): 2.0.12					
Use of Hard-coded	17-Oct-2022	9.8	go-admin (aka GO Admin) 2.0.12 uses the	N/A	A-GO--GO-A-041122/1492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Credentials			string go-admin as a production JWT key. **CVE ID : CVE-2022-42980**		
Vendor: Google					
Product: bazel					
Affected Version(s): From (including) 3.1.0 Up to (excluding) 4.2.3					
Insufficiently Protected Credentials	26-Oct-2022	4.3	A bad credential handling in the remote assets API for Bazel versions prior to 5.3.2 and 4.2.3 sends all user-provided credentials instead of only the required ones for the requests. We recommend upgrading to versions later than or equal to 5.3.2 or 4.2.3. **CVE ID : CVE-2022-3474**	https://github.com/bazelbuild/bazel/security/advisories/GHSA-mxr8-q875-rhwq	A-GOO-BAZE-041122/1493
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.3.2					
Insufficiently Protected Credentials	26-Oct-2022	4.3	A bad credential handling in the remote assets API for Bazel versions prior to 5.3.2 and 4.2.3 sends all user-provided credentials instead of only the required ones for the requests. We recommend upgrading to versions later than or equal to 5.3.2 or 4.2.3. **CVE ID : CVE-2022-3474**	https://github.com/bazelbuild/bazel/security/advisories/GHSA-mxr8-q875-rhwq	A-GOO-BAZE-041122/1494
Product: drive					
Affected Version(s): * Up to (excluding) 64.0					
Improper Privilege	17-Oct-2022	7.3	An attacker can pre-create the	https://support.google.co	A-GOO-DRIV-041122/1495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			`/Applications/Google\ Drive.app/Contents/MacOS` directory which is expected to be owned by root to be owned by a non-root user. When the Drive for Desktop installer is run for the first time, it will place a binary in that directory with execute permissions and set its setuid bit. Since the attacker owns the directory, the attacker can replace the binary with a symlink, causing the installer to set the setuid bit on the symlink. When the symlink is executed, it will run with root permissions. We recommend upgrading past version 64.0 **CVE ID : CVE-2022-3421**	m/a/answer/7577057?hl=en	
Vendor: gpac					
Product: gpac					
Affected Version(s): 2.1-dev-rev368-gfd054169b-master					
Out-of-bounds Write	19-Oct-2022	7.8	GPAC 2.1-DEV-rev368-gfd054169b-master was discovered to contain a heap buffer overflow via the function gf_isom_box_dump_start_ex at /isomedia/box_funcs.c. **CVE ID : CVE-2022-43040**	N/A	A-GPA-GPAC-041122/1496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2022	7.8	GPAC 2.1-DEV-rev368-gfd054169b-master was discovered to contain a heap buffer overflow via the function FixSDTPInTRAF at isomedia/isom_intern.c. **CVE ID : CVE-2022-43042**	N/A	A-GPA-GPAC-041122/1497
N/A	19-Oct-2022	5.5	GPAC 2.1-DEV-rev368-gfd054169b-master was discovered to contain a segmentation violation via the function gf_isom_meta_restore_items_ref at /isomedia/meta.c. **CVE ID : CVE-2022-43039**	N/A	A-GPA-GPAC-041122/1498
N/A	19-Oct-2022	5.5	GPAC 2.1-DEV-rev368-gfd054169b-master was discovered to contain a segmentation violation via the function BD_CheckSFTimeOffset at /bifs/field_decode.c. **CVE ID : CVE-2022-43043**	N/A	A-GPA-GPAC-041122/1499
N/A	19-Oct-2022	5.5	GPAC 2.1-DEV-rev368-gfd054169b-master was discovered to contain a segmentation violation via the function gf_isom_get_meta_item_info at /isomedia/meta.c. **CVE ID : CVE-2022-43044**	N/A	A-GPA-GPAC-041122/1500
N/A	19-Oct-2022	5.5	GPAC 2.1-DEV-rev368-gfd054169b-master was discovered to contain a segmentation violation	N/A	A-GPA-GPAC-041122/1501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via the function gf_dump_vrml_sffield at /scene_manager/scene_dump.c. **CVE ID : CVE-2022-43045**		
Vendor: Gradle					
Product: enterprise					
Affected Version(s): From (including) 2022.3 Up to (excluding) 2022.3.3					
Insufficiently Protected Credentials	21-Oct-2022	7.5	A credential-exposure vulnerability in the support-bundle mechanism in Gradle Enterprise 2022.3 through 2022.3.3 allows remote attackers to access a subset of application data (e.g., cleartext credentials). This is fixed in 2022.3.3. **CVE ID : CVE-2022-41575**	https://security.gradle.com/advisory/2022-13, https://security.gradle.com	A-GRA-ENTE-041122/1502
Vendor: hashicorp					
Product: boundary					
Affected Version(s): * Up to (excluding) 0.11.0					
Improper Restriction of Rendered UI Layers or Frames	27-Oct-2022	6.1	Hashicorp Boundary v0.8.0 is vulnerable to Clickjacking which allow for the interception of login credentials, re-direction of users to malicious sites, or causing users to perform malicious actions on the site. **CVE ID : CVE-2022-36182**	N/A	A-HAS-BOUN-041122/1503
Vendor: Haxx					
Product: curl					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 7.77.0 Up to (excluding) 7.86.0					
N/A	29-Oct-2022	0	curl before 7.86.0 has a double free. If curl is told to use an HTTP proxy for a transfer with a non-HTTP(S) URL, it sets up the connection to the remote server by issuing a CONNECT request to the proxy, and then tunnels the rest of the protocol through. An HTTP proxy might refuse this request (HTTP proxies often only allow outgoing connections to specific port numbers, like 443 for HTTPS) and instead return a non-200 status code to the client. Due to flaws in the error/cleanup handling, this could trigger a double free in curl if one of the following schemes were used in the URL for the transfer: dict, gopher, gophers, ldap, ldaps, rtmp, rtmps, or telnet. The earliest affected version is 7.77.0. **CVE ID : CVE-2022-42915**	N/A	A-HAX-CURL-041122/1504
Vendor: helpful_project					
Product: helpful					
Affected Version(s): * Up to (excluding) 4.5.26					
Exposure of Sensitive Informati on to an	17-Oct-2022	5.3	The Helpful WordPress plugin before 4.5.26 puts the exported logs and feedbacks in a publicly accessible location and guessable names, which	N/A	A-HEL-HELP-041122/1505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			could allow attackers to download them and retrieve sensitive information such as IP, Names and Email Address depending on the plugin's settings **CVE ID : CVE-2022-2834**		
Vendor: hiwin					
Product: robot_system_software					
Affected Version(s): 3.3.21.9869					
N/A	17-Oct-2022	7.5	HIWIN Robot System Software version 3.3.21.9869 does not properly address the terminated command source. As a result, an attacker could craft code to disconnect HRSS and the controller and cause a denial-of-service condition. **CVE ID : CVE-2022-3382**	N/A	A-HIW-ROBO-041122/1506
Vendor: hornerautomation					
Product: cscape					
Affected Version(s): * Up to (excluding) 9.90					
Out-of-bounds Write	27-Oct-2022	7.8	Horner Automation's Cscape version 9.90 SP7 and prior does not properly validate user-supplied data. If a user opens a maliciously formed FNT file, then an attacker could execute arbitrary code within the current process by writing outside the memory buffer.	N/A	A-HOR-CSCA-041122/1507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3379		
Access of Uninitialized Pointer	27-Oct-2022	7.8	Horner Automation's Cscape version 9.90 SP 7 and prior does not properly validate user-supplied data. If a user opens a maliciously formed FNT file, then an attacker could execute arbitrary code within the current process by accessing an uninitialized pointer, leading to an out-of-bounds memory write. **CVE ID : CVE-2022-3378**	N/A	A-HOR-CSCA-041122/1508
Affected Version(s): 9.90					
Out-of-bounds Write	27-Oct-2022	7.8	Horner Automation's Cscape version 9.90 SP7 and prior does not properly validate user-supplied data. If a user opens a maliciously formed FNT file, then an attacker could execute arbitrary code within the current process by writing outside the memory buffer. **CVE ID : CVE-2022-3379**	N/A	A-HOR-CSCA-041122/1509
Access of Uninitialized Pointer	27-Oct-2022	7.8	Horner Automation's Cscape version 9.90 SP 7 and prior does not properly validate user-supplied data. If a user opens a maliciously formed FNT file, then an attacker could execute arbitrary code within the	N/A	A-HOR-CSCA-041122/1510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current process by accessing an uninitialized pointer, leading to an out-of-bounds memory write. **CVE ID : CVE-2022-3378**		
Vendor: hospital_management_system_project					
Product: hospital_management_system					
Affected Version(s): 4.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	8.8	Hospital Management System v 4.0 is vulnerable to SQL Injection via file:hospital/hms/admin/view-patient.php. **CVE ID : CVE-2021-35387**	https://phpgurukul.com/hospital-management-system-in-php	A-HOS-HOSP-041122/1511
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-2022	5.4	PHPGurukul Hospital Management System In PHP V 4.0 is vulnerable to Cross Site Scripting (XSS) via add-patient.php. **CVE ID : CVE-2022-42205**	N/A	A-HOS-HOSP-041122/1512
Improper Neutralization of Input During Web Page Generation ('Cross-site	21-Oct-2022	5.4	PHPGurukul Hospital Management System In PHP V 4.0 is vulnerable to Cross Site Scripting (XSS) via doctor/view-patient.php, admin/view-patient.php, and view-medhistory.php.	N/A	A-HOS-HOSP-041122/1513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			**CVE ID : CVE-2022-42206**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-2022	5.4	Hospital Management System v 4.0 is vulnerable to Cross Site Scripting (XSS) via /hospital/hms/admin/patient-search.php. **CVE ID : CVE-2021-35388**	https://phpgurukul.com/hospital-management-system-in-php	A-HOS-HOSP-041122/1514
Vendor: hunter2_project					
Product: hunter2					
Affected Version(s): * Up to (excluding) 2.1.0					
Cleartext Storage of Sensitive Information	17-Oct-2022	6.5	An issue has been discovered in hunter2 affecting all versions before 2.1.0. Improper handling of auto-completion input allows an authenticated attacker to extract other users email addresses **CVE ID : CVE-2022-3540**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3540.json	A-HUN-HUNT-041122/1515
Vendor: IIJ					
Product: iij_smartkey					
Affected Version(s): * Up to (excluding) 2.1.4					
N/A	24-Oct-2022	7.5	Information disclosure vulnerability in Android App 'IIJ SmartKey' versions prior to 2.1.4 allows an attacker to obtain a one-time password issued by the product under certain conditions.	N/A	A-IIJ-IIJ_-041122/1516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41986		
Vendor: ikus-soft					
Product: rdiffweb					
Affected Version(s): * Up to (excluding) 2.4.10					
Missing Authentication for Critical Function	20-Oct-2022	9.8	Missing Authentication for Critical Function in GitHub repository ikus060/rdiffweb prior to 2.5.0a6. **CVE ID : CVE-2022-3327**	https://github.com/ikus060/rdiffweb/commit/f2a32f2a9f3fb8be1a9432ac3d81d3aacdb13095, https://huntr.dev/bounties/02207c8f-2b15-4a31-a86a-74fd2fca0ed1	A-IKU-RDIF-041122/1517
Affected Version(s): 2.4.10					
Missing Authentication for Critical Function	20-Oct-2022	9.8	Missing Authentication for Critical Function in GitHub repository ikus060/rdiffweb prior to 2.5.0a6. **CVE ID : CVE-2022-3327**	https://github.com/ikus060/rdiffweb/commit/f2a32f2a9f3fb8be1a9432ac3d81d3aacdb13095, https://huntr.dev/bounties/02207c8f-2b15-4a31-a86a-74fd2fca0ed1	A-IKU-RDIF-041122/1518
Affected Version(s): 2.5.0					
Missing Authentication for	20-Oct-2022	9.8	Missing Authentication for Critical Function in GitHub repository	https://github.com/ikus060/rdiffweb/commit/f	A-IKU-RDIF-041122/1519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			ikus060/rdiffweb prior to 2.5.0a6. **CVE ID : CVE-2022-3327**	2a32f2a9f3fb8be1a9432ac3d81d3aacdb13095, https://hunter.dev/bounties/02207c8f-2b15-4a31-a86a-74fd2fca0ed1	
Vendor: Ipfire					
Product: ipfire					
Affected Version(s): * Up to (excluding) 2.27					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Oct-2022	4.8	Multiple stored cross-site scripting vulnerabilities in the web user interface of IPFire versions prior to 2.27 allows a remote authenticated attacker with administrative privilege to inject an arbitrary script. **CVE ID : CVE-2022-36368**	https://blog.ipfire.org/post/ipfire-2-27-core-update-170-released, https://bugzilla.ipfire.org/show_bug.cgi?id=12925	A-IPF-IPFI-041122/1520
Affected Version(s): 2.27					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Oct-2022	4.8	Multiple stored cross-site scripting vulnerabilities in the web user interface of IPFire versions prior to 2.27 allows a remote authenticated attacker with administrative privilege to inject an arbitrary script. **CVE ID : CVE-2022-36368**	https://blog.ipfire.org/post/ipfire-2-27-core-update-170-released, https://bugzilla.ipfire.org/show_bug.cgi?id=12925	A-IPF-IPFI-041122/1521
Vendor: jadx_project					
Product: jadx					
Affected Version(s): * Up to (excluding) 1.4.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Oct-2022	5.5	jadx is a set of command line and GUI tools for producing Java source code from Android Dex and Apk files. versions prior to 1.4.5 are subject to a Denial of Service when opening zip files with HTML sequences. This issue has been patched in version 1.4.5. There are no known workarounds. **CVE ID : CVE-2022-39259**	https://github.com/skylot/jadx/security/advisories/GHSA-3r7j-8mqh-6qhx	A-JAD-JADX-041122/1522
Vendor: Jenkins					
Product: 360_fireline					
Affected Version(s): * Up to (including) 1.7.2					
N/A	19-Oct-2022	5.3	Jenkins 360 FireLine Plugin 1.7.2 and earlier programmatically disables Content-Security-Policy protection for user-generated content in workspaces, archived artifacts, etc. that Jenkins offers for download. **CVE ID : CVE-2022-43435**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2866	A-JEN-360_-041122/1523
Product: compuware_source_code_download_for_endevor\,_pds\,_and_ispw					
Affected Version(s): * Up to (excluding) 2.0.13					
N/A	19-Oct-2022	5.3	Jenkins Compuware Source Code Download for Endevor, PDS, and ISPW Plugin 2.0.12 and earlier implements an agent/controller message that does not limit where it can be executed, allowing	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2622	A-JEN-COMP-041122/1524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers able to control agent processes to obtain the values of Java system properties from the Jenkins controller process. **CVE ID : CVE-2022-43423**		
Product: compuware_strobe_measurement					
Affected Version(s): * Up to (including) 1.0.1					
Missing Authorization	19-Oct-2022	4.3	Jenkins Compuware Strobe Measurement Plugin 1.0.1 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. **CVE ID : CVE-2022-43431**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2631	A-JEN-COMP-041122/1525
Product: compuware_topax_for_total_test					
Affected Version(s): * Up to (including) 2.4.8					
Protection Mechanism Failure	19-Oct-2022	5.3	Jenkins Compuware Topaz for Total Test Plugin 2.4.8 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to obtain the values of Java system properties from the Jenkins controller process. **CVE ID : CVE-2022-43428**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2624	A-JEN-COMP-041122/1526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: compuware_topaz_for_total_test					
Affected Version(s): * Up to (including) 2.4.8					
Protection Mechanism Failure	19-Oct-2022	7.5	Jenkins Compuware Topaz for Total Test Plugin 2.4.8 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to read arbitrary files on the Jenkins controller file system. **CVE ID : CVE-2022-43429**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2624	A-JEN-COMP-041122/1527
Improper Restriction of XML External Entity Reference	19-Oct-2022	7.5	Jenkins Compuware Topaz for Total Test Plugin 2.4.8 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2022-43430**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2625	A-JEN-COMP-041122/1528
Missing Authorization	19-Oct-2022	4.3	Jenkins Compuware Topaz for Total Test Plugin 2.4.8 and earlier does not perform permission checks in several HTTP endpoints, allowing attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. **CVE ID : CVE-2022-43427**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2623	A-JEN-COMP-041122/1529
Product: compuware_topaz_utilities					
Affected Version(s): * Up to (excluding) 1.0.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Oct-2022	5.3	Jenkins Compuware Topaz Utilities Plugin 1.0.8 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to obtain the values of Java system properties from the Jenkins controller process. **CVE ID : CVE-2022-43422**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2620	A-JEN-COMP-041122/1530
Product: compuware_xpediter_code					
Affected Version(s): * Up to (including) 1.0.7					
Protection Mechanism Failure	19-Oct-2022	5.3	Jenkins Compuware Xpediter Code Coverage Plugin 1.0.7 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to obtain the values of Java system properties from the Jenkins controller process. **CVE ID : CVE-2022-43424**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2627	A-JEN-COMP-041122/1531
Product: contrast_continuous_application_security					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Input During	19-Oct-2022	5.4	Jenkins Contrast Continuous Application Security Plugin 3.9 and earlier does not escape data returned from the	https://www.jenkins.io/security/advisory/2022-10-	A-JEN-CONT-041122/1532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Contrast service when generating a report, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control or modify Contrast service API responses. **CVE ID : CVE-2022-43420**	19/#SECURITY-2836	
Product: custom_checkbox_parameter					
Affected Version(s): * Up to (including) 1.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2022	5.4	Jenkins Custom Checkbox Parameter Plugin 1.4 and earlier does not escape the name and description of Custom Checkbox Parameter parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission. **CVE ID : CVE-2022-43425**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2797	A-JEN-CUST-041122/1533
Product: generic_webhook_trigger					
Affected Version(s): * Up to (excluding) 1.84.2					
Observable Discrepancy	19-Oct-2022	5.3	Jenkins Generic Webhook Trigger Plugin 1.84.1 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2874	A-JEN-GENE-041122/1534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowing attackers to use statistical methods to obtain a valid webhook token. **CVE ID : CVE-2022-43412**		
Product: gitlab					
Affected Version(s): * Up to (excluding) 1.5.36					
Observable Discrepancy	19-Oct-2022	5.3	Jenkins GitLab Plugin 1.5.35 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token. **CVE ID : CVE-2022-43411**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2877	A-JEN-GITL-041122/1535
Product: groovy					
Affected Version(s): * Up to (including) 2802.v5ea_628154b_c2					
Protection Mechanism Failure	19-Oct-2022	9.9	A sandbox bypass vulnerability involving various casts performed implicitly by the Groovy language runtime in Jenkins Pipeline: Groovy Plugin 2802.v5ea_628154b_c2 and earlier allows attackers with permission to define and run sandboxed scripts, including Pipelines, to bypass the sandbox protection and execute arbitrary code in the	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2824%20(1)	A-JEN-GROO-041122/1536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the Jenkins controller JVM. **CVE ID : CVE-2022-43402**		
Product: groovy_libraries					
Affected Version(s): * Up to (including) 583.vf3b_454e43966					
Protection Mechanism Failure	19-Oct-2022	9.9	A sandbox bypass vulnerability in Jenkins Pipeline: Deprecated Groovy Libraries Plugin 583.vf3b_454e43966 and earlier allows attackers with permission to define untrusted Pipeline libraries and to define and run sandboxed scripts, including Pipelines, to bypass the sandbox protection and execute arbitrary code in the context of the Jenkins controller JVM. **CVE ID : CVE-2022-43406**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2824%20(2)	A-JEN-GROO-041122/1537
Affected Version(s): * Up to (including) 612.v84da_9c54906d					
N/A	19-Oct-2022	9.9	A sandbox bypass vulnerability in Jenkins Pipeline: Groovy Libraries Plugin 612.v84da_9c54906d and earlier allows attackers with permission to define untrusted Pipeline libraries and to define and run sandboxed scripts, including Pipelines, to bypass the sandbox protection and execute arbitrary code in	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2824%20(2)	A-JEN-GROO-041122/1538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the context of the Jenkins controller JVM. **CVE ID : CVE-2022-43405**		
Product: input_step					
Affected Version(s): * Up to (including) 451.vf1a_a_4f405289					
Inappropriate Encoding for Output Context	19-Oct-2022	8.8	Jenkins Pipeline: Input Step Plugin 451.vf1a_a_4f405289 and earlier does not restrict or sanitize the optionally specified ID of the 'input' step, which is used for the URLs that process user interactions for the given 'input' step (proceed or abort) and is not correctly encoded, allowing attackers able to configure Pipelines to have Jenkins build URLs from 'input' step IDs that would bypass the CSRF protection of any target URL in Jenkins when the 'input' step is interacted with. **CVE ID : CVE-2022-43407**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2880	A-JEN-INPU-041122/1539
Product: jenkins					
Affected Version(s): * Up to (including) 2.138					
N/A	19-Oct-2022	5.3	Jenkins Compuware Topaz Utilities Plugin 1.0.8 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to obtain	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2620	A-JEN-JENK-041122/1540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the values of Java system properties from the Jenkins controller process. **CVE ID : CVE-2022-43422**		
Affected Version(s): * Up to (including) 2.303.2					
N/A	19-Oct-2022	8.8	Jenkins Katalon Plugin 1.0.32 and earlier implements an agent/controller message that does not limit where it can be executed and allows invoking Katalon with configurable arguments, allowing attackers able to control agent processes to invoke Katalon on the Jenkins controller with attacker-controlled version, install location, and arguments, and attackers additionally able to create files on the Jenkins controller (e.g., attackers with Item/Configure permission could archive artifacts) to invoke arbitrary OS commands. **CVE ID : CVE-2022-43416**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2844	A-JEN-JENK-041122/1541
Protection Mechanism Failure	19-Oct-2022	7.5	Jenkins Compuware Topaz for Total Test Plugin 2.4.8 and earlier implements an agent/controller message that does not limit where it can be executed, allowing	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2624	A-JEN-JENK-041122/1542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers able to control agent processes to read arbitrary files on the Jenkins controller file system. **CVE ID : CVE-2022-43429**		
N/A	19-Oct-2022	5.3	Jenkins Compuware Topaz Utilities Plugin 1.0.8 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to obtain the values of Java system properties from the Jenkins controller process. **CVE ID : CVE-2022-43422**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2620	A-JEN-JENK-041122/1543
N/A	19-Oct-2022	5.3	Jenkins Compuware Source Code Download for Endevor, PDS, and ISPW Plugin 2.0.12 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to obtain the values of Java system properties from the Jenkins controller process. **CVE ID : CVE-2022-43423**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2622	A-JEN-JENK-041122/1544
Protection	19-Oct-2022	5.3	Jenkins Compuware Xpediter Code Coverage	https://www.jenkins.io/	A-JEN-JENK-041122/1545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Mechanism Failure			Plugin 1.0.7 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to obtain the values of Java system properties from the Jenkins controller process. **CVE ID : CVE-2022-43424**	security/advisory/2022-10-19/#SECURITY-2627	
Protection Mechanism Failure	19-Oct-2022	5.3	Jenkins Compuware Topaz for Total Test Plugin 2.4.8 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to obtain the values of Java system properties from the Jenkins controller process. **CVE ID : CVE-2022-43428**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2624	A-JEN-JENK-041122/1546
Affected Version(s): * Up to (including) 2.318					
N/A	19-Oct-2022	8.8	Jenkins Katalon Plugin 1.0.32 and earlier implements an agent/controller message that does not limit where it can be executed and allows invoking Katalon with configurable arguments, allowing attackers able to control agent	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2844	A-JEN-JENK-041122/1547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processes to invoke Katalon on the Jenkins controller with attacker-controlled version, install location, and arguments, and attackers additionally able to create files on the Jenkins controller (e.g., attackers with Item/Configure permission could archive artifacts) to invoke arbitrary OS commands. **CVE ID : CVE-2022-43416**		
Protection Mechanism Failure	19-Oct-2022	7.5	Jenkins Compuware Topaz for Total Test Plugin 2.4.8 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to read arbitrary files on the Jenkins controller file system. **CVE ID : CVE-2022-43429**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2624	A-JEN-JENK-041122/1548
N/A	19-Oct-2022	5.3	Jenkins Compuware Source Code Download for Endevor, PDS, and ISPW Plugin 2.0.12 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to obtain the values of Java system	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2622	A-JEN-JENK-041122/1549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			properties from the Jenkins controller process. **CVE ID : CVE-2022-43423**		
Protection Mechanism Failure	19-Oct-2022	5.3	Jenkins Compuware Xpediter Code Coverage Plugin 1.0.7 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to obtain the values of Java system properties from the Jenkins controller process. **CVE ID : CVE-2022-43424**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2627	A-JEN-JENK-041122/1550
Protection Mechanism Failure	19-Oct-2022	5.3	Jenkins Compuware Topaz for Total Test Plugin 2.4.8 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to obtain the values of Java system properties from the Jenkins controller process. **CVE ID : CVE-2022-43428**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2624	A-JEN-JENK-041122/1551
Product: job_import					
Affected Version(s): * Up to (excluding) 3.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	19-Oct-2022	4.3	Jenkins Job Import Plugin 3.5 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. **CVE ID : CVE-2022-43413**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2791	A-JEN-JOB_-041122/1552
Product: katalon					
Affected Version(s): * Up to (excluding) 1.0.33					
N/A	19-Oct-2022	8.8	Jenkins Katalon Plugin 1.0.32 and earlier implements an agent/controller message that does not limit where it can be executed and allows invoking Katalon with configurable arguments, allowing attackers able to control agent processes to invoke Katalon on the Jenkins controller with attacker-controlled version, install location, and arguments, and attackers additionally able to create files on the Jenkins controller (e.g., attackers with Item/Configure permission could archive artifacts) to invoke arbitrary OS commands. **CVE ID : CVE-2022-43416**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2844	A-JEN-KATA-041122/1553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	19-Oct-2022	6.5	Jenkins Katalon Plugin 1.0.32 and earlier stores API keys unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Extended Read permission, or access to the Jenkins controller file system. **CVE ID : CVE-2022-43419**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2846	A-JEN-KATA-041122/1554
Missing Authorization	19-Oct-2022	4.3	Jenkins Katalon Plugin 1.0.32 and earlier does not perform permission checks in several HTTP endpoints, allowing attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2022-43417**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2845%20(1)	A-JEN-KATA-041122/1555
Affected Version(s): * Up to (excluding) 1.0.34					
Cross-Site Request Forgery (CSRF)	19-Oct-2022	4.3	A cross-site request forgery (CSRF) vulnerability in Jenkins Katalon Plugin 1.0.33 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2845%20(2)	A-JEN-KATA-041122/1556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43418		
Product: mercurial					
Affected Version(s): * Up to (including) 1251.va_b_121f184902					
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	7.5	Jenkins Mercurial Plugin 1251.va_b_121f184902 and earlier provides information about which jobs were triggered or scheduled for polling through its webhook endpoint, including jobs the user has no permission to access. **CVE ID : CVE-2022-43410**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2831	A-JEN-MERC-041122/1557
Product: neuvector_vulnerability_scanner					
Affected Version(s): * Up to (including) 1.20					
Protection Mechanism Failure	19-Oct-2022	5.3	Jenkins NeuVector Vulnerability Scanner Plugin 1.20 and earlier programmatically disables Content-Security-Policy protection for user-generated content in workspaces, archived artifacts, etc. that Jenkins offers for download. **CVE ID : CVE-2022-43434**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2865	A-JEN-NEUV-041122/1558
Product: nunit					
Affected Version(s): * Up to (excluding) 0.28					
N/A	19-Oct-2022	5.3	Jenkins NUnit Plugin 0.27 and earlier implements an agent-to-controller message that parses files inside a user-specified directory as test results, allowing attackers able	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2551	A-JEN-NUNI-041122/1559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to control agent processes to obtain test results from files in an attacker-specified directory on the Jenkins controller. **CVE ID : CVE-2022-43414**		
Product: repo					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Restriction of XML External Entity Reference	19-Oct-2022	7.5	Jenkins REPO Plugin 1.15.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2022-43415**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2337	A-JEN-REPO-041122/1560
Product: s3_explorer					
Affected Version(s): * Up to (including) 1.0.8					
Missing Password Field Masking	19-Oct-2022	5.3	Jenkins S3 Explorer Plugin 1.0.8 and earlier does not mask the AWS_SECRET_ACCESS_KEY form field, increasing the potential for attackers to observe and capture it. **CVE ID : CVE-2022-43426**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2480	A-JEN-S3_E-041122/1561
Product: screenrecorder					
Affected Version(s): * Up to (including) 0.7					
Protection Mechanism Failure	19-Oct-2022	4.3	Jenkins ScreenRecorder Plugin 0.7 and earlier programmatically disables Content-Security-Policy protection for user-generated content in workspaces, archived	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2864	A-JEN-SCRE-041122/1562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			artifacts, etc. that Jenkins offers for download. **CVE ID : CVE-2022-43433**		
Product: script_security					
Affected Version(s): * Up to (including) 1183.v774b_0b_0a_a_451					
Protection Mechanism Failure	19-Oct-2022	9.9	A sandbox bypass vulnerability involving various casts performed implicitly by the Groovy language runtime in Jenkins Script Security Plugin 1183.v774b_0b_0a_a_451 and earlier allows attackers with permission to define and run sandboxed scripts, including Pipelines, to bypass the sandbox protection and execute arbitrary code in the context of the Jenkins controller JVM. **CVE ID : CVE-2022-43401**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2824%20(1)	A-JEN-SCRI-041122/1563
Protection Mechanism Failure	19-Oct-2022	9.9	A sandbox bypass vulnerability involving casting an array-like value to an array type in Jenkins Script Security Plugin 1183.v774b_0b_0a_a_451 and earlier allows attackers with permission to define and run sandboxed scripts, including Pipelines, to bypass the sandbox protection and execute arbitrary code in the	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2824%20(1)	A-JEN-SCRI-041122/1564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the Jenkins controller JVM. **CVE ID : CVE-2022-43403**		
Protection Mechanism Failure	19-Oct-2022	9.9	A sandbox bypass vulnerability involving crafted constructor bodies and calls to sandbox-generated synthetic constructors in Jenkins Script Security Plugin 1183.v774b_0b_0a_a_451 and earlier allows attackers with permission to define and run sandboxed scripts, including Pipelines, to bypass the sandbox protection and execute arbitrary code in the context of the Jenkins controller JVM. **CVE ID : CVE-2022-43404**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2824%20(1)	A-JEN-SCRI-041122/1565
Product: stage_view					
Affected Version(s): * Up to (including) 2.26					
Inappropriate Encoding for Output Context	19-Oct-2022	6.5	Jenkins Pipeline: Stage View Plugin 2.26 and earlier does not correctly encode the ID of 'input' steps when using it to generate URLs to proceed or abort Pipeline builds, allowing attackers able to configure Pipelines to specify 'input' step IDs resulting in URLs that would bypass the CSRF protection of any target URL in Jenkins.	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2828	A-JEN-STAG-051122/1566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43408		
Product: supporting_apis					
Affected Version(s): * Up to (including) 838.va_3a_087b_4055b					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2022	5.4	Jenkins Pipeline: Supporting APIs Plugin 838.va_3a_087b_4055b and earlier does not sanitize or properly encode URLs of hyperlinks sending POST requests in build logs, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to create Pipelines. **CVE ID : CVE-2022-43409**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2881	A-JEN-SUPP-051122/1567
Product: tuleap_git_branch_source					
Affected Version(s): * Up to (excluding) 3.2.5					
Missing Authorization	19-Oct-2022	5.3	A missing permission check in Jenkins Tuleap Git Branch Source Plugin 3.2.4 and earlier allows unauthenticated attackers to trigger Tuleap projects whose configured repository matches the attacker-specified value. **CVE ID : CVE-2022-43421**	https://www.jenkins.io/security/advisory/2022-10-19/#SECURITY-2852	A-JEN-TULE-051122/1568
Product: xframium_builder					
Affected Version(s): * Up to (including) 1.0.22					
N/A	19-Oct-2022	4.3	Jenkins XFramium Builder Plugin 1.0.22 and earlier programmatically disables Content-Security-Policy	https://www.jenkins.io/security/advisory/2022-10-	A-JEN-XFRA-051122/1569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protection for user-generated content in workspaces, archived artifacts, etc. that Jenkins offers for download. **CVE ID : CVE-2022-43432**	19/#SECURITY-2863	
Vendor: jflyfox					
Product: jfinal_cms					
Affected Version(s): 5.1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2022	8.8	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /admin/advicefeedback/list **CVE ID : CVE-2022-37202**	N/A	A-JFL-JFIN-051122/1570
Vendor: jhead_project					
Product: jhead					
Affected Version(s): 3.06.0.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Oct-2022	7.8	Jhead 3.06.0.1 allows attackers to execute arbitrary OS commands by placing them in a JPEG filename and then using the regeneration -rgt50 option. **CVE ID : CVE-2022-41751**	N/A	A-JHE-JHEA-051122/1571
Vendor: Joomla					
Product: joomla\!					
Affected Version(s): From (including) 4.0.0 Up to (including) 4.2.3					
Improper Neutraliz	25-Oct-2022	6.1	An issue was discovered in Joomla! 4.2.0 through	https://developer.joomla.	A-JOO-JOOM-051122/1572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation of Input During Web Page Generation ('Cross-site Scripting')			4.2.3. Inadequate filtering of potentially malicious user input leads to reflected XSS vulnerabilities in various components. **CVE ID : CVE-2022-27913**	org/security-centre/886-20221002-core-reflected-xss-in-various-components.html	
Exposure of Resource to Wrong Sphere	25-Oct-2022	5.3	An issue was discovered in Joomla! 4.0.0 through 4.2.3. Sites with publicly enabled debug mode exposed data of previous requests. **CVE ID : CVE-2022-27912**	https://developer.joomla.org/security-centre/885-20221001-core-disclosure-of-critical-information-in-debug-mode.html	A-JOO-JOOM-051122/1573
Vendor: jsonlint_project					
Product: jsonlint					
Affected Version(s): 1.0					
Out-of-bounds Write	19-Oct-2022	7.5	jsonlint 1.0 is vulnerable to heap-buffer-overflow via /home/hjsz/jsonlint/src/lexer. **CVE ID : CVE-2022-42227**	N/A	A-JSO-JSON-051122/1574
Vendor: Juiker					
Product: juiker					
Affected Version(s): 4.6.0311.1					
Use of Hard-coded Credentials	24-Oct-2022	6.1	Juiker app hard-coded its AES key in the source code. A physical attacker, after getting the Android root privilege, can use the AES key to decrypt	N/A	A-JUI-JUIK-051122/1575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users' ciphertext and tamper with it. **CVE ID : CVE-2022-38117**		
Vendor: Juniper					
Product: paragon_active_assurance_control_center					
Affected Version(s): * Up to (excluding) 3.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	8.4	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability, a stored XSS (or persistent), in the Control Center Controller web pages of Juniper Networks Paragon Active Assurance (Formerly Netrounds) allows a high-privilege attacker with 'WRITE' permissions to store one or more malicious scripts that will infect any other authorized user's account when they accidentally trigger the malicious script(s) while managing the device. Triggering these attacks enables the attacker to execute commands with the permissions up to that of the superuser account. This issue affects: Juniper Networks Paragon Active Assurance (Formerly Netrounds) All versions prior to 3.1.1; 3.2 versions prior to 3.2.1.	https://kb.juniper.net/JSA69883	A-JUN-PARA-051122/1576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22229		
Affected Version(s): 3.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	8.4	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability, a stored XSS (or persistent), in the Control Center Controller web pages of Juniper Networks Paragon Active Assurance (Formerly Netrounds) allows a high-privilege attacker with 'WRITE' permissions to store one or more malicious scripts that will infect any other authorized user's account when they accidentally trigger the malicious script(s) while managing the device. Triggering these attacks enables the attacker to execute commands with the permissions up to that of the superuser account. This issue affects: Juniper Networks Paragon Active Assurance (Formerly Netrounds) All versions prior to 3.1.1; 3.2 versions prior to 3.2.1. **CVE ID : CVE-2022-22229**	https://kb.juniper.net/JSA69883	A-JUN-PARA-051122/1577
Vendor: Jupyter					
Product: jupyter_core					
Affected Version(s): * Up to (including) 4.11.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	26-Oct-2022	8.8	Jupyter Core is a package for the core common functionality of Jupyter projects. Jupyter Core prior to version 4.11.2 contains an arbitrary code execution vulnerability in `jupyter_core` that stems from `jupyter_core` executing untrusted files in CWD. This vulnerability allows one user to run code as another. Version 4.11.2 contains a patch for this issue. There are no known workarounds. **CVE ID : CVE-2022-39286**	https://github.com/jupyter/jupyter_core/commit/1118c8ce01800cb689d51f655f5ccef19516e283, https://github.com/jupyter/jupyter_core/security/advisories/GHSA-m678-f26j-3hrp	A-JUP-JUPY-051122/1578
Vendor: kadencewp					
Product: kadence_woocommerce_email_designer					
Affected Version(s): * Up to (excluding) 1.5.7					
Deserialization of Untrusted Data	25-Oct-2022	7.2	The Kadence WooCommerce Email Designer WordPress plugin before 1.5.7 unserialises the content of an imported file, which could lead to PHP object injections issues when an admin import (intentionally or not) a malicious file and a suitable gadget chain is present on the blog. **CVE ID : CVE-2022-3335**	https://wpscan.com/vulnerability/39514705-c887-4a02-a77b-36e1dcca8f5d	A-KAD-KADE-051122/1579
Vendor: kartverket					
Product: github-workflows					
Affected Version(s): * Up to (excluding) 2.7.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	25-Oct-2022	8.8	kartverket/github-workflows are shared reusable workflows for GitHub Actions. Prior to version 2.7.5, all users of the `run-terraform` reusable workflow from the kartverket/github-workflows repo are affected by a code injection vulnerability. A malicious actor could potentially send a PR with a malicious payload leading to execution of arbitrary JavaScript code in the context of the workflow. Users should upgrade to at least version 2.7.5 to resolve the issue. As a workaround, review any pull requests from external users for malicious payloads before allowing them to trigger a build. **CVE ID : CVE-2022-39326**	https://github.com/kartverket/github-workflows/security/advisories/GHSA-f9qj-7gh3-mhj4, https://github.com/kartverket/github-workflows/pull/19, https://github.com/kartverket/github-workflows/releases/tag/v2.7.5	A-KAR-GITH-051122/1580
Vendor: keking					
Product: kkfileview					
Affected Version(s): 4.0.0					
Server-Side Request Forgery (SSRF)	17-Oct-2022	9.8	kkFileView 4.0 is vulnerable to Server-side request forgery (SSRF) via controller\OnlinePreviewController.java. **CVE ID : CVE-2022-42149**	N/A	A-KEK-KKFI-051122/1581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	6.1	kkFileView 4.0 is vulnerable to Cross Site Scripting (XSS) via controller\ Filecontroller.java. **CVE ID : CVE-2022-42147**	N/A	A-KEK-KKFI-051122/1582
Vendor: keystonejs					
Product: keystone					
Affected Version(s): From (including) 2.2.0 Up to (excluding) 2.3.1					
Incorrect Authorization	25-Oct-2022	9.8	@keystone-6/core is a core package for Keystone 6, a content management system for Node.js. Starting with version 2.2.0 and prior to version 2.3.1, users who expected their `multiselect` fields to use the field-level access control - if configured - are vulnerable to their field-level access control not being used. List-level access control is not affected. Field-level access control for fields other than `multiselect` are not affected. Version 2.3.1 contains a fix for this issue. As a workaround, stop using the `multiselect` field. **CVE ID : CVE-2022-39322**	https://github.com/keystonejs/keystone/security/advisories/GHSA-6mhr-52mv-6v6f, https://github.com/keystonejs/keystone/commit/65c6ee3def23605fc72b80230908696a7a65e7c	A-KEY-KEYS-051122/1583
Vendor: Laubrotel					
Product: lbstopattack					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.1.2					
Cross-Site Request Forgery (CSRF)	25-Oct-2022	6.5	The LBStopAttack WordPress plugin through 1.1.2 does not use nonces when saving its settings, making it possible for attackers to conduct CSRF attacks. This could allow attackers to disable the plugin's protections. **CVE ID : CVE-2022-3097**	N/A	A-LAU-LBST-051122/1584
Vendor: lavalite					
Product: lavalite					
Affected Version(s): 9.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2022	7.5	In Lavalite 9.0.0, the XSRF-TOKEN cookie is vulnerable to path traversal attacks, enabling read access to arbitrary files on the server. **CVE ID : CVE-2022-42188**	N/A	A-LAV-LAVA-051122/1585
Vendor: lemon8_project					
Product: lemon8					
Affected Version(s): * Up to (excluding) 3.3.5					
Incorrect Authorization	24-Oct-2022	6.5	Improper authorization in handler for custom URL scheme vulnerability in Lemon8 App for Android versions prior to 3.3.5 and Lemon8 App for iOS versions prior to 3.3.5 allows a remote attacker to lead a user to access an arbitrary website via	N/A	A-LEM-LEMO-051122/1586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the vulnerable App. As a result, the user may become a victim of a phishing attack. **CVE ID : CVE-2022-41797**		
Vendor: libexpat_project					
Product: libexpat					
Affected Version(s): * Up to (including) 2.4.9					
Use After Free	24-Oct-2022	7.5	In libexpat through 2.4.9, there is a use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate in out-of-memory situations. **CVE ID : CVE-2022-43680**	https://github.com/libexpat/libexpat/pull/650, https://github.com/libexpat/libexpat/pull/616, https://github.com/libexpat/libexpat/issues/649	A-LIB-LIBE-051122/1587
Vendor: Libtiff					
Product: libtiff					
Affected Version(s): * Up to (including) 4.4.0					
Out-of-bounds Write	21-Oct-2022	6.5	LibTIFF 4.4.0 has an out-of-bounds write in _TIFFmemcpy in libtiff/tif_unix.c:346 when called from extractImageSection, tools/tiffcrop.c:6826, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 236b7191. **CVE ID : CVE-2022-3597**	https://gitlab.com/libtiff/libtiff/-/issues/413, https://gitlab.com/libtiff/libtiff/-/commit/236b7191f04c60d09ee836ae13b50f812c841047, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE	A-LIB-LIBT-051122/1588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2022-3597.json	
Out-of-bounds Write	21-Oct-2022	6.5	LibTIFF 4.4.0 has an out-of-bounds write in extractContigSamplesShifted24bits in tools/tiffcrop.c:3604, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit cfbb883b. **CVE ID : CVE-2022-3598**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3598.json, https://gitlab.com/libtiff/libtiff/-/issues/435, https://gitlab.com/libtiff/libtiff/-/commit/cfbb883bf6ea7bedcb04177cc4e52d304522fdff	A-LIB-LIBT-051122/1589
Out-of-bounds Read	21-Oct-2022	6.5	LibTIFF 4.4.0 has an out-of-bounds read in writeSingleSection in tools/tiffcrop.c:7345, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit e8131125. **CVE ID : CVE-2022-3599**	https://gitlab.com/libtiff/libtiff/-/commit/e81311254594210755143 3d61afd16ac094ff246, https://gitlab.com/libtiff/libtiff/-/issues/398, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3599.json	A-LIB-LIBT-051122/1590
Out-of-bounds Write	21-Oct-2022	6.5	LibTIFF 4.4.0 has an out-of-bounds write in _TIFFmemset in	https://gitlab.com/gitlab-org/cves/-	A-LIB-LIBT-051122/1591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			libtiff/tif_unix.c:340 when called from processCropSelections, tools/tiffcrop.c:7619, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 236b7191. **CVE ID : CVE-2022-3626**	/blob/master/2022/CVE-2022-3626.json, https://gitlab.com/libtiff/libtiff/-/issues/426, https://gitlab.com/libtiff/libtiff/-/commit/236b7191f04c60d09ee836ae13b50f812c841047	
Out-of-bounds Write	21-Oct-2022	6.5	LibTIFF 4.4.0 has an out-of-bounds write in _TIFFmemcpy in libtiff/tif_unix.c:346 when called from extractImageSection, tools/tiffcrop.c:6860, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 236b7191. **CVE ID : CVE-2022-3627**	https://gitlab.com/libtiff/libtiff/-/commit/236b7191f04c60d09ee836ae13b50f812c841047, https://gitlab.com/libtiff/libtiff/-/issues/411, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3627.json	A-LIB-LIBT-051122/1592
Affected Version(s): From (including) 3.9.0 Up to (including) 4.4.0					
Out-of-bounds Write	21-Oct-2022	9.8	Multiple heap buffer overflows in tiffcrop.c utility in libtiff library Version 4.4.0 allows attacker to trigger unsafe or out of bounds memory access via crafted TIFF	https://gitlab.com/libtiff/libtiff/-/issues/386, https://gitlab.com/libtiff/libtiff/-	A-LIB-LIBT-051122/1593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			image file which could result into application crash, potential information disclosure or any other context-dependent impact **CVE ID : CVE-2022-3570**	/commit/bd94a9b383d8755a27b5a1bc27660b8ad10b094c, https://gitlab.com/libtiff/libtiff/-/issues/381	
Vendor: Liferay					
Product: dxp					
Affected Version(s): * Up to (excluding) 7.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	5.4	A Cross-site scripting (XSS) vulnerability in the Portal Search module's Sort widget in Liferay Portal 7.2.0 through 7.4.3.24, and Liferay DXP 7.2 before fix pack 19, 7.3 before update 5, and DXP 7.4 before update 25 allows remote attackers to inject arbitrary web script or HTML via a crafted payload. **CVE ID : CVE-2022-42112**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42112	A-LIF-DXP-051122/1594
Affected Version(s): * Up to (excluding) 7.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site scripting (XSS) vulnerability in the Frontend Editor module's integration with CKEditor in Liferay Portal 7.3.2 through 7.4.3.14, and Liferay DXP 7.3 before update 6, and 7.4 before update 15 allows remote attackers to inject arbitrary web script or HTML via the	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42116	A-LIF-DXP-051122/1595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(1) name, or (2) namespace parameter. **CVE ID : CVE-2022-42116**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site scripting (XSS) vulnerability in the Frontend Taglib module in Liferay Portal 7.3.2 through 7.4.3.16, and Liferay DXP 7.3 before update 6, and 7.4 before update 17 allows remote attackers to inject arbitrary web script or HTML. **CVE ID : CVE-2022-42117**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42117	A-LIF-DXP-051122/1596
Affected Version(s): * Up to (excluding) 7.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	5.4	A Cross-site scripting (XSS) vulnerability in the Role module's edit role assignees page in Liferay Portal 7.4.0 through 7.4.3.36, and Liferay DXP 7.4 before update 37 allows remote attackers to inject arbitrary web script or HTML. **CVE ID : CVE-2022-42114**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42114	A-LIF-DXP-051122/1597
Affected Version(s): 7.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site	18-Oct-2022	5.4	A Cross-site scripting (XSS) vulnerability in the Portal Search module's Sort widget in Liferay Portal 7.2.0 through 7.4.3.24, and Liferay DXP 7.2 before fix pack 19, 7.3 before update 5, and DXP 7.4 before update 25 allows remote attackers	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/c	A-LIF-DXP-051122/1598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			to inject arbitrary web script or HTML via a crafted payload. **CVE ID : CVE-2022-42112**	ontent/cve-2022-42112	
Affected Version(s): 7.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site scripting (XSS) vulnerability in the Frontend Editor module's integration with CKEditor in Liferay Portal 7.3.2 through 7.4.3.14, and Liferay DXP 7.3 before update 6, and 7.4 before update 15 allows remote attackers to inject arbitrary web script or HTML via the (1) name, or (2) namespace parameter. **CVE ID : CVE-2022-42116**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42116	A-LIF-DXP-051122/1599
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site scripting (XSS) vulnerability in the Frontend Taglib module in Liferay Portal 7.3.2 through 7.4.3.16, and Liferay DXP 7.3 before update 6, and 7.4 before update 17 allows remote attackers to inject arbitrary web script or HTML. **CVE ID : CVE-2022-42117**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42117	A-LIF-DXP-051122/1600
Improper Neutralization of Input During Web Page Generatio	19-Oct-2022	5.4	A Cross-site scripting (XSS) vulnerability in the Document and Media module - file upload functionality in Liferay Digital Experience Platform 7.3.10 SP3	http://liferay.com	A-LIF-DXP-051122/1601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n ('Cross-site Scripting')			allows remote attackers to inject arbitrary JS script or HTML into the description field of uploaded svg file. **CVE ID : CVE-2022-38901**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	5.4	A Cross-site scripting (XSS) vulnerability in the Portal Search module's Sort widget in Liferay Portal 7.2.0 through 7.4.3.24, and Liferay DXP 7.2 before fix pack 19, 7.3 before update 5, and DXP 7.4 before update 25 allows remote attackers to inject arbitrary web script or HTML via a crafted payload. **CVE ID : CVE-2022-42112**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42112	A-LIF-DXP-051122/1602
Affected Version(s): 7.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site scripting (XSS) vulnerability in Document Library module in Liferay Portal 7.4.3.30 through 7.4.3.36, and Liferay DXP 7.4 update 30 through update 36 allows remote attackers to inject arbitrary web script or HTML via the `redirect` parameter. **CVE ID : CVE-2022-42113**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42113	A-LIF-DXP-051122/1603
Improper Neutralization of Input During	18-Oct-2022	6.1	A Cross-site scripting (XSS) vulnerability in the Frontend Editor module's integration with CKEditor in Liferay	https://portal.liferay.dev/learn/security/known-vulnerabiliti	A-LIF-DXP-051122/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Portal 7.3.2 through 7.4.3.14, and Liferay DXP 7.3 before update 6, and 7.4 before update 15 allows remote attackers to inject arbitrary web script or HTML via the (1) name, or (2) namespace parameter. **CVE ID : CVE-2022-42116**	es/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42116	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site scripting (XSS) vulnerability in the Frontend Taglib module in Liferay Portal 7.3.2 through 7.4.3.16, and Liferay DXP 7.3 before update 6, and 7.4 before update 17 allows remote attackers to inject arbitrary web script or HTML. **CVE ID : CVE-2022-42117**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42117	A-LIF-DXP-051122/1605
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2022	5.4	A Cross-site scripting (XSS) vulnerability in the Document and Media module - file upload functionality in Liferay Digital Experience Platform 7.3.10 SP3 allows remote attackers to inject arbitrary JS script or HTML into the description field of uploaded svg file. **CVE ID : CVE-2022-38901**	http://liferay.com	A-LIF-DXP-051122/1606
Improper Neutralization of Input	18-Oct-2022	5.4	A Cross-site scripting (XSS) vulnerability in the Portal Search module's Sort widget in Liferay	https://portal.liferay.dev/learn/security/known-	A-LIF-DXP-051122/1607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Portal 7.2.0 through 7.4.3.24, and Liferay DXP 7.2 before fix pack 19, 7.3 before update 5, and DXP 7.4 before update 25 allows remote attackers to inject arbitrary web script or HTML via a crafted payload. **CVE ID : CVE-2022-42112**	vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42112	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	5.4	A Cross-site scripting (XSS) vulnerability in the Role module's edit role assignees page in Liferay Portal 7.4.0 through 7.4.3.36, and Liferay DXP 7.4 before update 37 allows remote attackers to inject arbitrary web script or HTML. **CVE ID : CVE-2022-42114**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42114	A-LIF-DXP-051122/1608
Affected Version(s): From (including) 7.0 Up to (excluding) 7.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2022	5.4	A Cross-site scripting (XSS) vulnerability in the Document and Media module - file upload functionality in Liferay Digital Experience Platform 7.3.10 SP3 allows remote attackers to inject arbitrary JS script or HTML into the description field of uploaded svg file. **CVE ID : CVE-2022-38901**	http://liferay.com	A-LIF-DXP-051122/1609
Product: liferay_portal					
Affected Version(s): From (including) 7.2.0 Up to (excluding) 7.4.3.25					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	5.4	A Cross-site scripting (XSS) vulnerability in the Portal Search module's Sort widget in Liferay Portal 7.2.0 through 7.4.3.24, and Liferay DXP 7.2 before fix pack 19, 7.3 before update 5, and DXP 7.4 before update 25 allows remote attackers to inject arbitrary web script or HTML via a crafted payload. **CVE ID : CVE-2022-42112**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42112	A-LIF-LIFE-051122/1610
Affected Version(s): From (including) 7.3.2 Up to (excluding) 7.4.3.15					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site scripting (XSS) vulnerability in the Frontend Editor module's integration with CKEditor in Liferay Portal 7.3.2 through 7.4.3.14, and Liferay DXP 7.3 before update 6, and 7.4 before update 15 allows remote attackers to inject arbitrary web script or HTML via the (1) name, or (2) namespace parameter. **CVE ID : CVE-2022-42116**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42116	A-LIF-LIFE-051122/1611
Affected Version(s): From (including) 7.3.2 Up to (including) 7.4.3.16					
Improper Neutralization of Input During Web Page Generation ('Cross-site	18-Oct-2022	6.1	A Cross-site scripting (XSS) vulnerability in the Frontend Taglib module in Liferay Portal 7.3.2 through 7.4.3.16, and Liferay DXP 7.3 before update 6, and 7.4 before update 17 allows remote attackers to inject	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/c	A-LIF-LIFE-051122/1612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			arbitrary web script or HTML. **CVE ID : CVE-2022-42117**	ontent/cve-2022-42117	
Affected Version(s): From (including) 7.3.5 Up to (including) 7.4.3.28					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2022	5.4	A Cross-site scripting (XSS) vulnerability in the Document and Media module - file upload functionality in Liferay Digital Experience Platform 7.3.10 SP3 allows remote attackers to inject arbitrary JS script or HTML into the description field of uploaded svg file. **CVE ID : CVE-2022-38901**	http://liferay.com	A-LIF-LIFE-051122/1613
Affected Version(s): From (including) 7.4.0 Up to (excluding) 7.4.3.37					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	5.4	A Cross-site scripting (XSS) vulnerability in the Role module's edit role assignees page in Liferay Portal 7.4.0 through 7.4.3.36, and Liferay DXP 7.4 before update 37 allows remote attackers to inject arbitrary web script or HTML. **CVE ID : CVE-2022-42114**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42114	A-LIF-LIFE-051122/1614
Affected Version(s): From (including) 7.4.3.30 Up to (excluding) 7.4.3.37					
Improper Neutralization of Input During Web Page Generation ('Cross-	18-Oct-2022	6.1	A Cross-site scripting (XSS) vulnerability in Document Library module in Liferay Portal 7.4.3.30 through 7.4.3.36, and Liferay DXP 7.4 update 30 through update 36 allows remote	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5m	A-LIF-LIFE-051122/1615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
site Scripting')			attackers to inject arbitrary web script or HTML via the `redirect` parameter. **CVE ID : CVE-2022-42113**	xmVrnXW/content/cve-2022-42113	
Affected Version(s): From (including) 7.4.3.4 Up to (excluding) 7.4.3.37					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	5.4	Cross-site scripting (XSS) vulnerability in the Object module's edit object details page in Liferay Portal 7.4.3.4 through 7.4.3.36 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into the object field's `Label` text field. **CVE ID : CVE-2022-42115**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42115	A-LIF-LIFE-051122/1616
Vendor: Litespeedtech					
Product: openlitespeed					
Affected Version(s): 1.5.11					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Oct-2022	5.8	Directory Traversal vulnerability in LiteSpeed Technologies OpenLiteSpeed Web Server Dashboard allows Path Traversal. This affects versions from 1.5.11 through 1.5.12, from 1.6.5 through 1.6.20.1, from 1.7.0 before 1.7.16.1 **CVE ID : CVE-2022-0072**	N/A	A-LIT-OPEN-051122/1617
Affected Version(s): 1.5.12					
Improper Limitatio	27-Oct-2022	5.8	Directory Traversal vulnerability in	N/A	A-LIT-OPEN-051122/1618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n of a Pathname to a Restricted Directory ('Path Traversal')			LiteSpeed Technologies OpenLiteSpeed Web Server Dashboard allows Path Traversal. This affects versions from 1.5.11 through 1.5.12, from 1.6.5 through 1.6.20.1, from 1.7.0 before 1.7.16.1 **CVE ID : CVE-2022-0072**		
Affected Version(s): From (including) 1.6.15 Up to (excluding) 1.7.16.1					
Untrusted Search Path	27-Oct-2022	8.8	Untrusted Search Path vulnerability in LiteSpeed Technologies OpenLiteSpeed Web Server Container allows Privilege Escalation. This affects versions from 1.6.15 before 1.7.16.1. **CVE ID : CVE-2022-0074**	N/A	A-LIT-OPEN-051122/1619
Affected Version(s): From (including) 1.6.5 Up to (including) 1.6.20.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Oct-2022	5.8	Directory Traversal vulnerability in LiteSpeed Technologies OpenLiteSpeed Web Server Dashboard allows Path Traversal. This affects versions from 1.5.11 through 1.5.12, from 1.6.5 through 1.6.20.1, from 1.7.0 before 1.7.16.1 **CVE ID : CVE-2022-0072**	N/A	A-LIT-OPEN-051122/1620
Affected Version(s): From (including) 1.7.0 Up to (excluding) 1.7.16.1					
Improper Limitation of a Pathname	27-Oct-2022	5.8	Directory Traversal vulnerability in LiteSpeed Technologies OpenLiteSpeed Web	N/A	A-LIT-OPEN-051122/1621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Server Dashboard allows Path Traversal. This affects versions from 1.5.11 through 1.5.12, from 1.6.5 through 1.6.20.1, from 1.7.0 before 1.7.16.1 **CVE ID : CVE-2022-0072**		
Affected Version(s): From (including) 1.7.0 Up to (including) 1.7.16.1					
Improper Input Validation	27-Oct-2022	8.8	Improper Input Validation vulnerability in LiteSpeed Technologies OpenLiteSpeed Web Server Dashboard allows Command Injection. This affects 1.7.0 versions before 1.7.16.1. **CVE ID : CVE-2022-0073**	N/A	A-LIT-OPEN-051122/1622
Vendor: Magento					
Product: magento					
Affected Version(s): * Up to (excluding) 2.3.7					
Improper Input Validation	20-Oct-2022	8.8	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an improper input validation vulnerability. An authenticated attacker can trigger an insecure direct object reference in the `V1/customers/me` endpoint to achieve information exposure and privilege escalation. **CVE ID : CVE-2022-42344**	https://helpx.adobe.com/security/products/magento/apsb22-38.html	A-MAG-MAGE-051122/1623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.3.7					
Improper Input Validation	20-Oct-2022	8.8	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an improper input validation vulnerability. An authenticated attacker can trigger an insecure direct object reference in the `V1/customers/me` endpoint to achieve information exposure and privilege escalation. **CVE ID : CVE-2022-42344**	https://helpx.adobe.com/security/products/magento/apsb22-38.html	A-MAG-MAGE-051122/1624
Affected Version(s): 2.4.3					
Improper Input Validation	20-Oct-2022	8.8	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an improper input validation vulnerability. An authenticated attacker can trigger an insecure direct object reference in the `V1/customers/me` endpoint to achieve information exposure and privilege escalation. **CVE ID : CVE-2022-42344**	https://helpx.adobe.com/security/products/magento/apsb22-38.html	A-MAG-MAGE-051122/1625
Affected Version(s): 2.4.4					
Improper Input Validation	20-Oct-2022	8.8	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by	https://helpx.adobe.com/security/products/mag	A-MAG-MAGE-051122/1626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an improper input validation vulnerability. An authenticated attacker can trigger an insecure direct object reference in the `V1/customers/me` endpoint to achieve information exposure and privilege escalation. **CVE ID : CVE-2022-42344**	ento/apsb22-38.html	
Affected Version(s): From (including) 2.4.0 Up to (excluding) 2.4.3					
Improper Input Validation	20-Oct-2022	8.8	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an improper input validation vulnerability. An authenticated attacker can trigger an insecure direct object reference in the `V1/customers/me` endpoint to achieve information exposure and privilege escalation. **CVE ID : CVE-2022-42344**	https://helpx.adobe.com/security/products/magento/apsb22-38.html	A-MAG-MAGE-051122/1627
Vendor: markdownify_project					
Product: markdownify					
Affected Version(s): 1.4.1					
N/A	19-Oct-2022	7.8	Markdownify version 1.4.1 allows an external attacker to execute arbitrary code remotely on any client attempting to view a malicious markdown file through Markdownify. This is	N/A	A-MAR-MARK-051122/1628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible because the application has the "nodeIntegration" option enabled. **CVE ID : CVE-2022-41709**		
Vendor: Mcafee					
Product: epolicy_orchestrator					
Affected Version(s): * Up to (excluding) 5.10.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A reflected cross-site scripting (XSS) vulnerability in ePO prior to 5.10 Update 14 allows a remote unauthenticated attacker to potentially obtain access to an ePO administrator's session by convincing the authenticated ePO administrator to click on a carefully crafted link. This would lead to limited access to sensitive information and limited ability to alter some information in ePO. **CVE ID : CVE-2022-3339**	https://kcm.trellix.com/corporate/index?page=content&id=SB10387	A-MCA-EPOL-051122/1629
Improper Restriction of XML External Entity Reference	18-Oct-2022	5.4	An External XML entity (XXE) vulnerability in ePO prior to 5.10 Update 14 can lead to an unauthenticated remote attacker to potentially trigger a Server Side Request Forgery attack. This can be exploited by mimicking the Agent Handler call to ePO and passing the carefully	https://kcm.trellix.com/corporate/index?page=content&id=SB10387	A-MCA-EPOL-051122/1630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			constructed XML file through the API. **CVE ID : CVE-2022-3338**		
Affected Version(s): 5.10.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A reflected cross-site scripting (XSS) vulnerability in ePO prior to 5.10 Update 14 allows a remote unauthenticated attacker to potentially obtain access to an ePO administrator's session by convincing the authenticated ePO administrator to click on a carefully crafted link. This would lead to limited access to sensitive information and limited ability to alter some information in ePO. **CVE ID : CVE-2022-3339**	https://kcm.trellix.com/corporate/index?page=content&id=SB10387	A-MCA-EPOL-051122/1631
Improper Restriction of XML External Entity Reference	18-Oct-2022	5.4	An External XML entity (XXE) vulnerability in ePO prior to 5.10 Update 14 can lead to an unauthenticated remote attacker to potentially trigger a Server Side Request Forgery attack. This can be exploited by mimicking the Agent Handler call to ePO and passing the carefully constructed XML file through the API. **CVE ID : CVE-2022-3338**	https://kcm.trellix.com/corporate/index?page=content&id=SB10387	A-MCA-EPOL-051122/1632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: megazone					
Product: reversewall-mds					
Affected Version(s): * Up to (excluding) 3.8_a008					
Improper Authentication	17-Oct-2022	9.8	Remote code execution vulnerability due to insufficient user privilege verification in reverseWall-MDS. Remote attackers can exploit the vulnerability such as stealing account, through remote code execution. **CVE ID : CVE-2022-23769**	N/A	A-MEG-REVE-051122/1633
Vendor: mekshq					
Product: meks_easy_social_share					
Affected Version(s): * Up to (excluding) 1.2.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	4.8	The Meks Easy Social Share WordPress plugin before 1.2.8 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2574**	N/A	A-MEK-MEKS-051122/1634
Vendor: merchandise_online_store_project					
Product: merchandise_online_store					
Affected Version(s): 1.0					
Improper Neutraliz	17-Oct-2022	9.8	A SQL Injection issue in Merchandise Online	N/A	A-MER-MERC-051122/1635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation of Special Elements used in an SQL Command ('SQL Injection')			Store v.1.0 allows an attacker to log in to the admin account. **CVE ID : CVE-2022-42237**		
Vendor: metabase					
Product: metabase					
Affected Version(s): * Up to (excluding) 0.44.5					
Server-Side Request Forgery (SSRF)	26-Oct-2022	6.5	The url parameter of the /api/geojson endpoint in Metabase versions <44.5 can be used to perform Server Side Request Forgery attacks. Previously implemented blacklists could be circumvented by leveraging 301 and 302 redirects. **CVE ID : CVE-2022-43776**	N/A	A-MET-META-051122/1636
Affected Version(s): From (including) 0.41.0 Up to (excluding) 0.41.9					
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, H2 (Sample Database) could allow Remote Code Execution (RCE), which can be abused by users able to write SQL queries on H2 databases. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer	https://github.com/metabase/metabase/security/advisories/GHSA-gqpj-wcr3-p88v	A-MET-META-051122/1637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows DDL statements in H2 native queries. **CVE ID : CVE-2022-39361**		
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, unsaved SQL queries are auto-executed, which could pose a possible attack vector. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer automatically executes ad-hoc native queries. Now the native editor shows the query and gives the user the option to manually run the query if they want. **CVE ID : CVE-2022-39362**	https://github.com/metabase/metabase/commit/b7c6bb905a9187347cfc9035443b514713027a5c, https://github.com/metabase/metabase/security/advisories/GHSA-93wj-fgjg-r238	A-MET-META-051122/1638
URL Redirection to Untrusted Site ('Open Redirect')	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, custom GeoJSON map URL address would follow redirects to addresses that were otherwise disallowed, like link-local or private-network. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6,	https://github.com/metabase/metabase/security/advisories/GHSA-w5j7-4mgm-77f4, https://github.com/metabase/metabase/commit/057e2d67fcbeb6b48db68b697e022	A-MET-META-051122/1639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.41.9, and 1.41.9. Metabase no longer follow redirects on GeoJSON map URLs. An environment variable `MB_CUSTOM_GEOJSON_ENABLED` was also added to disable custom GeoJSON completely (`true` by default). **CVE ID : CVE-2022-39359**	243e3a5771e	
Improper Authentication	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9 single sign on (SSO) users were able to do password resets on Metabase, which could allow a user access without going through the SSO IdP. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase now blocks password reset for all users who use SSO for their Metabase login. **CVE ID : CVE-2022-39360**	https://github.com/metabase/metabase/commit/edadf7303c3b068609f57ca073e67885d5c98730, https://github.com/metabase/metabase/security/advisories/GHSA-gw4g-ww2m-v7vc	A-MET-META-051122/1640
Affected Version(s): From (including) 0.42.0 Up to (excluding) 0.42.6					
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, H2 (Sample Database) could allow	https://github.com/metabase/metabase/security/advisories/GHSA-gqpj-wcr3-p88v	A-MET-META-051122/1641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution (RCE), which can be abused by users able to write SQL queries on H2 databases. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer allows DDL statements in H2 native queries. **CVE ID : CVE-2022-39361**		
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, unsaved SQL queries are auto-executed, which could pose a possible attack vector. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer automatically executes ad-hoc native queries. Now the native editor shows the query and gives the user the option to manually run the query if they want. **CVE ID : CVE-2022-39362**	https://github.com/metabase/metabase/commit/b7c6bb905a9187347cfc9035443b514713027a5c, https://github.com/metabase/metabase/security/advisories/GHSA-93wj-fgjg-r238	A-MET-META-051122/1642
Improper Locking	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, and 1.42.6, it was	https://github.com/metabase/metabase/security/advisories	A-MET-META-051122/1643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible to circumvent locked parameters when requesting data for a question in an embedded dashboard by constructing a malicious request to the backend. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, and 1.42.6. **CVE ID : CVE-2022-39358**	/GHSA-8qgm-9mj6-36h3	
URL Redirection to Untrusted Site ('Open Redirect')	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, custom GeoJSON map URL address would follow redirects to addresses that were otherwise disallowed, like link-local or private-network. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer follow redirects on GeoJSON map URLs. An environment variable `MB_CUSTOM_GEOJSON_ENABLED` was also added to disable custom GeoJSON completely (`true` by default). **CVE ID : CVE-2022-39359**	https://github.com/metabase/metabase/security/advisories/GHSA-w5j7-4mgm-77f4, https://github.com/metabase/metabase/commit/057e2d67fcbeb6b48db68b697e022243e3a5771e	A-MET-META-051122/1644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9 single sign on (SSO) users were able to do password resets on Metabase, which could allow a user access without going through the SSO IdP. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase now blocks password reset for all users who use SSO for their Metabase login. **CVE ID : CVE-2022-39360**	https://github.com/metabase/metabase/commit/edadf7303c3b068609f57ca073e67885d5c98730, https://github.com/metabase/metabase/security/advisories/GHSA-gw4g-ww2m-v7vc	A-MET-META-051122/1645
Affected Version(s): From (including) 0.43.0 Up to (excluding) 0.43.7					
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, H2 (Sample Database) could allow Remote Code Execution (RCE), which can be abused by users able to write SQL queries on H2 databases. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer allows DDL statements in H2 native queries.	https://github.com/metabase/metabase/security/advisories/GHSA-gqpj-wcr3-p88v	A-MET-META-051122/1646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39361		
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, unsaved SQL queries are auto-executed, which could pose a possible attack vector. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer automatically executes ad-hoc native queries. Now the native editor shows the query and gives the user the option to manually run the query if they want. **CVE ID : CVE-2022-39362**	https://github.com/metabase/metabase/commit/b7c6bb905a9187347cfc9035443b514713027a5c, https://github.com/metabase/metabase/security/advisories/GHSA-93wj-fgjg-r238	A-MET-META-051122/1647
Improper Locking	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, and 1.42.6, it was possible to circumvent locked parameters when requesting data for a question in an embedded dashboard by constructing a malicious request to the backend. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, and 1.42.6.	https://github.com/metabase/metabase/security/advisories/GHSA-8qgm-9mj6-36h3	A-MET-META-051122/1648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39358		
URL Redirection to Untrusted Site ('Open Redirect')	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, custom GeoJSON map URL address would follow redirects to addresses that were otherwise disallowed, like link-local or private-network. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer follow redirects on GeoJSON map URLs. An environment variable `MB_CUSTOM_GEOJSON_ENABLED` was also added to disable custom GeoJSON completely (`true` by default). **CVE ID : CVE-2022-39359**	https://github.com/metabase/metabase/security/advisories/GHSA-w5j7-4mgm-77f4, https://github.com/metabase/metabase/commit/057e2d67fcbeb6b48db68b697e022243e3a5771e	A-MET-META-051122/1649
Improper Authentication	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9 single sign on (SSO) users were able to do password resets on Metabase, which could allow a user access without going through the SSO IdP. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7,	https://github.com/metabase/metabase/commit/edadf7303c3b068609f57ca073e67885d5c98730, https://github.com/metabase/metabase/security/advisories	A-MET-META-051122/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase now blocks password reset for all users who use SSO for their Metabase login. **CVE ID : CVE-2022-39360**	/GHSA-gw4g-ww2m-v7vc	
Affected Version(s): From (including) 0.44.0 Up to (excluding) 0.44.5					
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, H2 (Sample Database) could allow Remote Code Execution (RCE), which can be abused by users able to write SQL queries on H2 databases. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer allows DDL statements in H2 native queries. **CVE ID : CVE-2022-39361**	https://github.com/metabase/metabase/security/advisories/GHSA-gqpj-wcr3-p88v	A-MET-META-051122/1651
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, unsaved SQL queries are auto-executed, which could pose a possible attack vector. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7,	https://github.com/metabase/metabase/commit/b7c6bb905a9187347cfc9035443b514713027a5c, https://github.com/metabase/meta	A-MET-META-051122/1652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer automatically executes ad-hoc native queries. Now the native editor shows the query and gives the user the option to manually run the query if they want. **CVE ID : CVE-2022-39362**	base/security/advisories/GHSA-93wj-fgjg-r238	
Improper Locking	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, and 1.42.6, it was possible to circumvent locked parameters when requesting data for a question in an embedded dashboard by constructing a malicious request to the backend. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, and 1.42.6. **CVE ID : CVE-2022-39358**	https://github.com/metabase/metabase/security/advisories/GHSA-8qgm-9mj6-36h3	A-MET-META-051122/1653
URL Redirection to Untrusted Site ('Open Redirect')	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, custom GeoJSON map URL address would follow redirects to addresses that were otherwise disallowed, like link-local or private-network. This issue is patched in versions	https://github.com/metabase/metabase/security/advisories/GHSA-w5j7-4mgm-77f4, https://github.com/metabase/metabase/commit/057e2d67f	A-MET-META-051122/1654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer follow redirects on GeoJSON map URLs. An environment variable `MB_CUSTOM_GEOJSON_ENABLED` was also added to disable custom GeoJSON completely (`true` by default). **CVE ID : CVE-2022-39359**	cbeb6b48db68b697e022243e3a5771e	
Improper Authentication	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9 single sign on (SSO) users were able to do password resets on Metabase, which could allow a user access without going through the SSO IdP. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase now blocks password reset for all users who use SSO for their Metabase login. **CVE ID : CVE-2022-39360**	https://github.com/metabase/metabase/commit/edadf7303c3b068609f57ca073e67885d5c98730, https://github.com/metabase/metabase/security/advisories/GHSA-gw4g-ww2m-v7vc	A-MET-META-051122/1655
Affected Version(s): From (including) 1.41.0 Up to (excluding) 1.41.9					
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and	https://github.com/metabase/metabase/security/advisories	A-MET-META-051122/1656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.41.9, H2 (Sample Database) could allow Remote Code Execution (RCE), which can be abused by users able to write SQL queries on H2 databases. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer allows DDL statements in H2 native queries. **CVE ID : CVE-2022-39361**	/GHSA-gqpj-wcr3-p88v	
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, unsaved SQL queries are auto-executed, which could pose a possible attack vector. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer automatically executes ad-hoc native queries. Now the native editor shows the query and gives the user the option to manually run the query if they want. **CVE ID : CVE-2022-39362**	https://github.com/metabase/metabase/commit/b7c6bb905a9187347cfc9035443b514713027a5c, https://github.com/metabase/metabase/security/advisories/GHSA-93wj-fgjg-r238	A-MET-META-051122/1657
URL Redirection to	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5,	https://github.com/metabase/meta	A-MET-META-051122/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Site ('Open Redirect')			1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, custom GeoJSON map URL address would follow redirects to addresses that were otherwise disallowed, like link-local or private-network. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer follow redirects on GeoJSON map URLs. An environment variable `MB_CUSTOM_GEOJSON_ENABLED` was also added to disable custom GeoJSON completely (`true` by default). **CVE ID : CVE-2022-39359**	base/security/advisories/GHSA-w5j7-4mgm-77f4, https://github.com/metabase/metabase/commit/057e2d67fcbeb6b48db68b697e022243e3a5771e	
Improper Authentication	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9 single sign on (SSO) users were able to do password resets on Metabase, which could allow a user access without going through the SSO IdP. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase now blocks password reset for all	https://github.com/metabase/metabase/commit/edadf7303c3b068609f57ca073e67885d5c98730, https://github.com/metabase/metabase/security/advisories/GHSA-gw4g-ww2m-v7vc	A-MET-META-051122/1659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users who use SSO for their Metabase login. **CVE ID : CVE-2022-39360**		
Affected Version(s): From (including) 1.42.0 Up to (excluding) 1.42.6					
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, H2 (Sample Database) could allow Remote Code Execution (RCE), which can be abused by users able to write SQL queries on H2 databases. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer allows DDL statements in H2 native queries. **CVE ID : CVE-2022-39361**	https://github.com/metabase/metabase/security/advisories/GHSA-gqpj-wcr3-p88v	A-MET-META-051122/1660
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, unsaved SQL queries are auto-executed, which could pose a possible attack vector. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer automatically executes	https://github.com/metabase/metabase/commit/b7c6bb905a9187347cfc9035443b514713027a5c, https://github.com/metabase/metabase/security/advisories/GHSA-	A-MET-META-051122/1661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ad-hoc native queries. Now the native editor shows the query and gives the user the option to manually run the query if they want. **CVE ID : CVE-2022-39362**	93wj-fgjg-r238	
Improper Locking	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, and 1.42.6, it was possible to circumvent locked parameters when requesting data for a question in an embedded dashboard by constructing a malicious request to the backend. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, and 1.42.6. **CVE ID : CVE-2022-39358**	https://github.com/metabase/metabase/security/advisories/GHSA-8qgm-9mj6-36h3	A-MET-META-051122/1662
URL Redirection to Untrusted Site ('Open Redirect')	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, custom GeoJSON map URL address would follow redirects to addresses that were otherwise disallowed, like link-local or private-network. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer	https://github.com/metabase/metabase/security/advisories/GHSA-w5j7-4mgm-77f4, https://github.com/metabase/metabase/commit/057e2d67fcbeb6b48db68b697e022	A-MET-META-051122/1663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			follow redirects on GeoJSON map URLs. An environment variable `MB_CUSTOM_GEOJSON_ENABLED` was also added to disable custom GeoJSON completely (`true` by default). **CVE ID : CVE-2022-39359**	243e3a5771e	
Improper Authentication	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9 single sign on (SSO) users were able to do password resets on Metabase, which could allow a user access without going through the SSO IdP. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase now blocks password reset for all users who use SSO for their Metabase login. **CVE ID : CVE-2022-39360**	https://github.com/metabase/metabase/commit/edadf7303c3b068609f57ca073e67885d5c98730, https://github.com/metabase/metabase/security/advisories/GHSA-gw4g-ww2m-v7vc	A-MET-META-051122/1664
Affected Version(s): From (including) 1.43.0 Up to (excluding) 1.43.7					
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, H2 (Sample Database) could allow Remote Code Execution (RCE), which can be	https://github.com/metabase/metabase/security/advisories/GHSA-gqpj-wcr3-p88v	A-MET-META-051122/1665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			abused by users able to write SQL queries on H2 databases. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer allows DDL statements in H2 native queries. **CVE ID : CVE-2022-39361**		
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, unsaved SQL queries are auto-executed, which could pose a possible attack vector. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer automatically executes ad-hoc native queries. Now the native editor shows the query and gives the user the option to manually run the query if they want. **CVE ID : CVE-2022-39362**	https://github.com/metabase/metabase/commit/b7c6bb905a9187347cfc9035443b514713027a5c, https://github.com/metabase/metabase/security/advisories/GHSA-93wj-fgjg-r238	A-MET-META-051122/1666
Improper Locking	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, and 1.42.6, it was possible to circumvent locked parameters when	https://github.com/metabase/metabase/security/advisories/GHSA-	A-MET-META-051122/1667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requesting data for a question in an embedded dashboard by constructing a malicious request to the backend. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, and 1.42.6. **CVE ID : CVE-2022-39358**	8qgm-9mj6-36h3	
URL Redirection to Untrusted Site ('Open Redirect')	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, custom GeoJSON map URL address would follow redirects to addresses that were otherwise disallowed, like link-local or private-network. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer follow redirects on GeoJSON map URLs. An environment variable `MB_CUSTOM_GEOJSON_ENABLED` was also added to disable custom GeoJSON completely (`true` by default). **CVE ID : CVE-2022-39359**	https://github.com/metabase/metabase/security/advisories/GHSA-w5j7-4mgm-77f4, https://github.com/metabase/metabase/commit/057e2d67fcbeb6b48db68b697e022243e3a5771e	A-MET-META-051122/1668
Improper Authentication	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and	https://github.com/metabase/metabase/commit/edadf7303	A-MET-META-051122/1669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.41.9 single sign on (SSO) users were able to do password resets on Metabase, which could allow a user access without going through the SSO IdP. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase now blocks password reset for all users who use SSO for their Metabase login. **CVE ID : CVE-2022-39360**	c3b068609f57ca073e67885d5c98730, https://github.com/metabase/metabase/security/advisories/GHSA-gw4g-ww2m-v7vc	
Affected Version(s): From (including) 1.44.0 Up to (excluding) 1.44.5					
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, H2 (Sample Database) could allow Remote Code Execution (RCE), which can be abused by users able to write SQL queries on H2 databases. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer allows DDL statements in H2 native queries. **CVE ID : CVE-2022-39361**	https://github.com/metabase/metabase/security/advisories/GHSA-gqpj-wcr3-p88v	A-MET-META-051122/1670
N/A	26-Oct-2022	8.8	Metabase is data visualization software. Prior to versions 0.44.5,	https://github.com/metabase/meta	A-MET-META-051122/1671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9, unsaved SQL queries are auto-executed, which could pose a possible attack vector. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer automatically executes ad-hoc native queries. Now the native editor shows the query and gives the user the option to manually run the query if they want. **CVE ID : CVE-2022-39362**	base/commit/b7c6bb905a9187347cfc9035443b514713027a5c, https://github.com/metabase/metabase/security/advisories/GHSA-93wj-fgjg-r238	
Improper Locking	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, and 1.42.6, it was possible to circumvent locked parameters when requesting data for a question in an embedded dashboard by constructing a malicious request to the backend. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, and 1.42.6. **CVE ID : CVE-2022-39358**	https://github.com/metabase/metabase/security/advisories/GHSA-8qgm-9mj6-36h3	A-MET-META-051122/1672
URL Redirection to Untrusted	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7,	https://github.com/metabase/metabase/securit	A-MET-META-051122/1673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			0.42.6, 1.42.6, 0.41.9, and 1.41.9, custom GeoJSON map URL address would follow redirects to addresses that were otherwise disallowed, like link-local or private-network. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase no longer follow redirects on GeoJSON map URLs. An environment variable `MB_CUSTOM_GEOJSON_ENABLED` was also added to disable custom GeoJSON completely (`true` by default). **CVE ID : CVE-2022-39359**	y/advisories/GHSA-w5j7-4mgm-77f4, https://github.com/metabase/metabase/commit/057e2d67fcbeb6b48db68b697e022243e3a5771e	
Improper Authentication	26-Oct-2022	6.5	Metabase is data visualization software. Prior to versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9 single sign on (SSO) users were able to do password resets on Metabase, which could allow a user access without going through the SSO IdP. This issue is patched in versions 0.44.5, 1.44.5, 0.43.7, 1.43.7, 0.42.6, 1.42.6, 0.41.9, and 1.41.9. Metabase now blocks password reset for all users who use SSO for their Metabase login.	https://github.com/metabase/metabase/commit/edadf7303c3b068609f57ca073e67885d5c98730, https://github.com/metabase/metabase/security/advisories/GHSA-gw4g-ww2m-v7vc	A-MET-META-051122/1674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39360		
Vendor: Microsoft					
Product: azure_command-line_interface					
Affected Version(s): * Up to (excluding) 2.40.0					
Improper Control of Generation of Code ('Code Injection')	25-Oct-2022	9.8	Azure CLI is the command-line interface for Microsoft Azure. In versions previous to 2.40.0, Azure CLI contains a vulnerability for potential code injection. Critical scenarios are where a hosting machine runs an Azure CLI command where parameter values have been provided by an external source. The vulnerability is only applicable when the Azure CLI command is run on a Windows machine and with any version of PowerShell and when the parameter value contains the `&` or `|` symbols. If any of these prerequisites are not met, this vulnerability is not applicable. Users should upgrade to version 2.40.0 or greater to receive a a mitigation for the vulnerability. **CVE ID : CVE-2022-39327**	https://github.com/Azure/azure-cli/security/advisories/GHSA-47xc-9rr2-q7p4, https://github.com/Azure/azure-cli/pull/23514, https://github.com/Azure/azure-cli/pull/24015	A-MIC-AZUR-051122/1675
Vendor: mindskip					
Product: xzs					
Affected Version(s): 3.8.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	5.4	xzs v3.8.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the component /admin/question/edit. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title text field. **CVE ID : CVE-2022-41431**	N/A	A-MIN-XZS-051122/1676
Vendor: minimatch_project					
Product: minimatch					
Affected Version(s): * Up to (excluding) 3.0.5					
N/A	17-Oct-2022	7.5	A vulnerability was found in the minimatch package. This flaw allows a Regular Expression Denial of Service (ReDoS) when calling the braceExpand function with specific arguments, resulting in a Denial of Service. **CVE ID : CVE-2022-3517**	https://github.com/grafana/grafana-image-renderer/issues/329, https://github.com/isaacs/minimatch/commit/a8763f4388e51956be62dc6025cec1126beeb5e6	A-MIN-MINI-051122/1677
Vendor: miniorange					
Product: discord_integration					
Affected Version(s): * Up to (excluding) 2.1.6					
Cross-Site Request Forgery (CSRF)	17-Oct-2022	6.5	The miniOrange Discord Integration WordPress plugin before 2.1.6 does not have authorisation and CSRF in some of its AJAX actions, allowing any logged in users, such	N/A	A-MIN-DISC-051122/1678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as subscriber to call them, and disable the app for example **CVE ID : CVE-2022-3082**		
Vendor: Mitel					
Product: micollab					
Affected Version(s): * Up to (excluding) 9.6					
Unrestricted Upload of File with Dangerous Type	25-Oct-2022	9.8	A vulnerability in the web conferencing component of Mitel MiCollab through 9.5.0.101 could allow an unauthenticated attacker to upload malicious files. A successful exploit could allow an attacker to execute arbitrary code within the context of the application. **CVE ID : CVE-2022-36452**	https://www.mitel.com/support/security-advisories	A-MIT-MICO-051122/1679
Affected Version(s): * Up to (including) 9.5.0.101					
Server-Side Request Forgery (SSRF)	25-Oct-2022	8.8	A vulnerability in the MiCollab Client server component of Mitel MiCollab through 9.5.0.101 could allow an authenticated attacker to conduct a Server-Side Request Forgery (SSRF) attack due to insufficient restriction of URL parameters. A successful exploit could allow an attacker to leverage connections and permissions available to the host server. **CVE ID : CVE-2022-36451**	https://www.mitel.com/support/security-advisories, https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-22-0006	A-MIT-MICO-051122/1680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Oct-2022	6.5	A vulnerability in the MiCollab Client API of Mitel MiCollab through 9.5.0.101 could allow an authenticated attacker to modify their profile parameters due to improper authorization controls. A successful exploit could allow the authenticated attacker to impersonate another user's name. **CVE ID : CVE-2022-36454**	https://www.mitel.com/support/security-advisories, https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-22-0006	A-MIT-MICO-051122/1681
Affected Version(s): From (including) 9.1.3 Up to (including) 9.5.0.101					
N/A	25-Oct-2022	8.8	A vulnerability in the MiCollab Client API of Mitel MiCollab 9.1.3 through 9.5.0.101 could allow an authenticated attacker to modify their profile parameters due to improper authorization controls. A successful exploit could allow the authenticated attacker to control another extension number. **CVE ID : CVE-2022-36453**	https://www.mitel.com/support/security-advisories, https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-22-0006	A-MIT-MICO-051122/1682
Vendor: Mitre					
Product: caldera					
Affected Version(s): * Up to (excluding) 4.1.0					
Improper Neutralization of Input During Web Page Generatio	17-Oct-2022	6.1	MITRE CALDERA before 4.1.0 allows XSS in the Operations tab and/or Debrief plugin via a crafted operation name, a different vulnerability than CVE-2022-40606.	N/A	A-MIT-CALD-051122/1683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n ('Cross-site Scripting')			**CVE ID : CVE-2022-40605**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	6.1	MITRE CALDERA before 4.1.0 allows XSS in the Operations tab and/or Debrief plugin via a crafted operation name, a different vulnerability than CVE-2022-40605. **CVE ID : CVE-2022-40606**	N/A	A-MIT-CALD-051122/1684
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	5.4	MITRE CALDERA 4.1.0 allows stored XSS via app.contact.gist (aka the gist contact configuration field), leading to execution of arbitrary commands on agents. **CVE ID : CVE-2022-41139**	N/A	A-MIT-CALD-051122/1685
Vendor: Najeebmedia					
Product: frontend_file_manager_plugin					
Affected Version(s): * Up to (excluding) 21.4					
Cross-Site Request Forgery (CSRF)	17-Oct-2022	4.3	The Frontend File Manager Plugin WordPress plugin before 21.4 does not have CSRF check when uploading files, which could allow attackers to make logged in users upload files on their behalf **CVE ID : CVE-2022-3126**	N/A	A-NAJ-FRON-051122/1686
Vendor: Nextcloud					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nextcloud_enterprise_server					
Affected Version(s): * Up to (excluding) 22.2.10.5					
Cleartext Storage of Sensitive Information	27-Oct-2022	6.5	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. In Nextcloud Server prior to versions 23.0.9 and 24.0.5 and Nextcloud Enterprise Server prior to versions 22.2.10.5, 23.0.9, and 24.0.5 an attacker reading `nextcloud.log` may gain knowledge of credentials to connect to a SharePoint service. Nextcloud Server versions 23.0.9 and 24.0.5 and Nextcloud Enterprise Server versions 22.2.10.5, 23.0.9, and 24.0.5 contain a patch for this issue. As a workaround, set `zend.exception_ignore_args = On` as an option in `php.ini`. **CVE ID : CVE-2022-39364**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-qpf5-jj85-36h5,https://github.com/nextcloud/server/pull/33689	A-NEX-NEXT-051122/1687
Affected Version(s): * Up to (excluding) 23.0.9					
Incorrect Authorization	27-Oct-2022	5.3	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. Nextcloud Server and Nextcloud Enterprise Server prior to versions 23.0.9 and 24.0.5 are vulnerable to exposure of information that cannot be controlled by	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8f3p-rcm5-mrg3,https://github.com/nextcloud/	A-NEX-NEXT-051122/1688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrators without direct database access. Versions 23.0.9 and 24.0.5 contains patches for this issue. No known workarounds are available. **CVE ID : CVE-2022-39329**	server/pull/33643	
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.9					
Cleartext Storage of Sensitive Information	27-Oct-2022	6.5	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. In Nextcloud Server prior to versions 23.0.9 and 24.0.5 and Nextcloud Enterprise Server prior to versions 22.2.10.5, 23.0.9, and 24.0.5 an attacker reading `nextcloud.log` may gain knowledge of credentials to connect to a SharePoint service. Nextcloud Server versions 23.0.9 and 24.0.5 and Nextcloud Enterprise Server versions 22.2.10.5, 23.0.9, and 24.0.5 contain a patch for this issue. As a workaround, set `zend.exception_ignore_args = On` as an option in `php.ini`. **CVE ID : CVE-2022-39364**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-qpf5-jj85-36h5,https://github.com/nextcloud/server/pull/33689	A-NEX-NEXT-051122/1689
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.5					
Cleartext Storage of Sensitive	27-Oct-2022	6.5	Nextcloud Server is the file server software for Nextcloud, a self-hosted	https://github.com/nextcloud/securi	A-NEX-NEXT-051122/1690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			productivity platform. In Nextcloud Server prior to versions 23.0.9 and 24.0.5 and Nextcloud Enterprise Server prior to versions 22.2.10.5, 23.0.9, and 24.0.5 an attacker reading `nextcloud.log` may gain knowledge of credentials to connect to a SharePoint service. Nextcloud Server versions 23.0.9 and 24.0.5 and Nextcloud Enterprise Server versions 22.2.10.5, 23.0.9, and 24.0.5 contain a patch for this issue. As a workaround, set `zend.exception_ignore_args = On` as an option in `php.ini`. **CVE ID : CVE-2022-39364**	ty-advisories/security/advisories/GHSA-qpf5-jj85-36h5,https://github.com/nextcloud/server/pull/33689	
Incorrect Authorization	27-Oct-2022	5.3	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. Nextcloud Server and Nextcloud Enterprise Server prior to versions 23.0.9 and 24.0.5 are vulnerable to exposure of information that cannot be controlled by administrators without direct database access. Versions 23.0.9 and 24.0.5 contains patches for this issue. No known workarounds are available.	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8f3p-rcm5-mrg3,https://github.com/nextcloud/server/pull/33643	A-NEX-NEXT-051122/1691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39329		
Product: nextcloud_server					
Affected Version(s): * Up to (excluding) 23.0.9					
Cleartext Storage of Sensitive Information	27-Oct-2022	6.5	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. In Nextcloud Server prior to versions 23.0.9 and 24.0.5 and Nextcloud Enterprise Server prior to versions 22.2.10.5, 23.0.9, and 24.0.5 an attacker reading `nextcloud.log` may gain knowledge of credentials to connect to a SharePoint service. Nextcloud Server versions 23.0.9 and 24.0.5 and Nextcloud Enterprise Server versions 22.2.10.5, 23.0.9, and 24.0.5 contain a patch for this issue. As a workaround, set `zend.exception_ignore_args = On` as an option in `php.ini`. **CVE ID : CVE-2022-39364**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-qpf5-jj85-36h5,https://github.com/nextcloud/server/pull/33689	A-NEX-NEXT-051122/1692
Incorrect Authorization	27-Oct-2022	5.3	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. Nextcloud Server and Nextcloud Enterprise Server prior to versions 23.0.9 and 24.0.5 are vulnerable to exposure of information that cannot	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8f3p-rcm5-mrg3,https://github.com	A-NEX-NEXT-051122/1693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be controlled by administrators without direct database access. Versions 23.0.9 and 24.0.5 contains patches for this issue. No known workarounds are available. **CVE ID : CVE-2022-39329**	/nextcloud/server/pull/33643	
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.5					
Cleartext Storage of Sensitive Information	27-Oct-2022	6.5	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. In Nextcloud Server prior to versions 23.0.9 and 24.0.5 and Nextcloud Enterprise Server prior to versions 22.2.10.5, 23.0.9, and 24.0.5 an attacker reading `nextcloud.log` may gain knowledge of credentials to connect to a SharePoint service. Nextcloud Server versions 23.0.9 and 24.0.5 and Nextcloud Enterprise Server versions 22.2.10.5, 23.0.9, and 24.0.5 contain a patch for this issue. As a workaround, set `zend.exception_ignore_args = On` as an option in `php.ini`. **CVE ID : CVE-2022-39364**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-qpf5-jj85-36h5,https://github.com/nextcloud/server/pull/33689	A-NEX-NEXT-051122/1694
Incorrect Authorization	27-Oct-2022	5.3	Nextcloud Server is the file server software for Nextcloud, a self-hosted	https://github.com/nextcloud/securi	A-NEX-NEXT-051122/1695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			productivity platform. Nextcloud Server and Nextcloud Enterprise Server prior to versions 23.0.9 and 24.0.5 are vulnerable to exposure of information that cannot be controlled by administrators without direct database access. Versions 23.0.9 and 24.0.5 contains patches for this issue. No known workarounds are available. **CVE ID : CVE-2022-39329**	ty-advisories/security/advisories/GHSA-8f3p-rcm5-mrg3,https://github.com/nextcloud/server/pull/33643	
Vendor: nopcommerce					
Product: nopcommerce					
Affected Version(s): * Up to (including) 4.50.2					
Authorization Bypass Through User-Controlled Key	19-Oct-2022	7.5	An access control issue in nopcommerce v4.50.2 allows attackers to arbitrarily modify any customer's address via the addressedit endpoint. **CVE ID : CVE-2022-33077**	http://nopcommerce.com	A-NOP-NOPC-051122/1696
Affected Version(s): From (including) 4.10 Up to (excluding) 4.50.2					
URL Redirection to Untrusted Site ('Open Redirect')	20-Oct-2022	6.1	Multiple open redirect vulnerabilities in NopCommerce 4.10 through 4.50.1 allow remote attackers to conduct phishing attacks by redirecting users to attacker-controlled web sites via the returnUrl parameter, processed by the (1) ChangePassword function, (2)	https://gist.github.com/adeadfed/baea45138b7eb29e09f6505d56b56413	A-NOP-NOPC-051122/1697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SignInCustomerAsync function, (3) SuccessfulAuthentication method, or (4) NopRedirectResultExecutor class. **CVE ID : CVE-2022-26954**		
Vendor: ocomon_project					
Product: ocomon					
Affected Version(s): 4.0					
N/A	19-Oct-2022	7.5	OcoMon 4.0RC1 is vulnerable to Incorrect Access Control. Through a request the user can obtain the real email, sending the same request with correct email its possible to account takeover. **CVE ID : CVE-2022-40798**	N/A	A-OCO-OCOM-051122/1698
Affected Version(s): * Up to (excluding) 4.0					
N/A	19-Oct-2022	7.5	OcoMon 4.0RC1 is vulnerable to Incorrect Access Control. Through a request the user can obtain the real email, sending the same request with correct email its possible to account takeover. **CVE ID : CVE-2022-40798**	N/A	A-OCO-OCOM-051122/1699
Vendor: octoprint					
Product: octoprint					
Affected Version(s): * Up to (excluding) 1.8.3					
Improper Neutraliz	19-Oct-2022	6	Failure to Sanitize Special Elements into a	https://hunt r.dev/bounti	A-OCT-OCTO-051122/1700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation of Special Elements in Output Used by a Downstream Component ('Injection')			Different Plane (Special Element Injection) in GitHub repository octoprint/octoprint prior to 1.8.3. **CVE ID : CVE-2022-3607**	es/2d1db3c9-93e8-4902-a55b-5ea53c22aa11, https://github.com/octoprint/octoprint/commit/3cca3a43f3d085e9bbe5a5840c8255bb1b5d052e	
Vendor: octopus					
Product: octopus_server					
Affected Version(s): * Up to (excluding) 2022.1.3264					
Generation of Error Message Containing Sensitive Information	27-Oct-2022	5.3	In affected versions of Octopus Server it is possible to reveal the existence of resources in a space that the user does not have access to due to verbose error messaging. **CVE ID : CVE-2022-2508**	https://advisories.octopus.com/post/2022/sa2022-22/	A-OCT-OCTO-051122/1701
Affected Version(s): * Up to (excluding) 2022.2.8351					
Insufficient Session Expiration	27-Oct-2022	9.1	In affected versions of Octopus Server it is possible for a session token to be valid indefinitely due to improper validation of the session token parameters. **CVE ID : CVE-2022-2782**	https://advisories.octopus.com/post/2022/sa2022-21/	A-OCT-OCTO-051122/1702
Affected Version(s): From (including) 2022.2.0 Up to (excluding) 2022.2.8351					
Generation of Error Message	27-Oct-2022	5.3	In affected versions of Octopus Server it is possible to reveal the	https://advisories.octopus.com/post	A-OCT-OCTO-051122/1703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Containing Sensitive Information			existence of resources in a space that the user does not have access to due to verbose error messaging. **CVE ID : CVE-2022-2508**	/2022/sa2022-22/	
Affected Version(s): From (including) 2022.3.0 Up to (excluding) 2022.3.10586					
Insufficient Session Expiration	27-Oct-2022	9.1	In affected versions of Octopus Server it is possible for a session token to be valid indefinitely due to improper validation of the session token parameters. **CVE ID : CVE-2022-2782**	https://advisories.octopus.com/post/2022/sa2022-21/	A-OCT-OCTO-051122/1704
Generation of Error Message Containing Sensitive Information	27-Oct-2022	5.3	In affected versions of Octopus Server it is possible to reveal the existence of resources in a space that the user does not have access to due to verbose error messaging. **CVE ID : CVE-2022-2508**	https://advisories.octopus.com/post/2022/sa2022-22/	A-OCT-OCTO-051122/1705
Affected Version(s): From (including) 2022.4.0 Up to (excluding) 2022.4.2898					
Insufficient Session Expiration	27-Oct-2022	9.1	In affected versions of Octopus Server it is possible for a session token to be valid indefinitely due to improper validation of the session token parameters. **CVE ID : CVE-2022-2782**	https://advisories.octopus.com/post/2022/sa2022-21/	A-OCT-OCTO-051122/1706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Error Message Containing Sensitive Information	27-Oct-2022	5.3	In affected versions of Octopus Server it is possible to reveal the existence of resources in a space that the user does not have access to due to verbose error messaging. **CVE ID : CVE-2022-2508**	https://advisories.octopus.com/post/2022/sa2022-22/	A-OCT-OCTO-051122/1707
Vendor: online_medicine_ordering_system_project					
Product: online_medicine_ordering_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Oct-2022	9.8	A vulnerability classified as critical has been found in SourceCodester Online Medicine Ordering System 1.0. Affected is an unknown function of the file admin/?page=orders/view_order. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. VDB-212346 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3714**	N/A	A-ONL-ONLI-051122/1708
Improper Neutralization of Input During Web Page Generation ('Cross-site	27-Oct-2022	5.4	A vulnerability classified as problematic was found in SourceCodester Online Medicine Ordering System 1.0. Affected by this vulnerability is an unknown functionality of the file /omos/admin/?page=user/list. The manipulation	N/A	A-ONL-ONLI-051122/1709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			of the argument First Name/Middle Name/Last Name leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-212347. **CVE ID : CVE-2022-3716**		
Vendor: online_pet_shop_we_app_project					
Product: online_pet_shop_we_app					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	27-Oct-2022	7.2	Online Pet Shop We App v1.0 was discovered to contain an arbitrary file upload vulnerability via the Editing function in the User module. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file uploaded through the picture upload point. **CVE ID : CVE-2022-39977**	N/A	A-ONL-ONLI-051122/1710
Unrestricted Upload of File with Dangerous Type	27-Oct-2022	7.2	Online Pet Shop We App v1.0 was discovered to contain an arbitrary file upload vulnerability via the Editing function in the Product List module. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file uploaded through the picture upload point.	N/A	A-ONL-ONLI-051122/1711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39978		
Vendor: online_tours_and_travels_management_system_project					
Product: online_tours_and_travels_management_system					
Affected Version(s): 1.0					
N/A	17-Oct-2022	7.2	Online Tours & Travels Management System v1.0 is vulnerable to Arbitrary code execution via ip/tour/admin/operations/update_settings.php. **CVE ID : CVE-2022-42142**	N/A	A-ONL-ONLI-051122/1712
Vendor: online_tours_\&_travels_management_system_project					
Product: online_tours_\&_travels_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	18-Oct-2022	7.2	Online Tours & Travels Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via the component /user_operations/profile.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-41537**	N/A	A-ONL-ONLI-051122/1713
Vendor: Open-xchange					
Product: ox_app_suite					
Affected Version(s): * Up to (including) 7.10.6					
Improper Neutralization of Special Elements used in an OS	25-Oct-2022	9.8	documentconverter in OX App Suite through 7.10.6, in a non-default configuration with ghostscript, allows OS Command Injection because file conversion	N/A	A-OPE-OX_A-051122/1714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			may occur for an EPS document that is disguised as a PDF document. **CVE ID : CVE-2022-29851**		
Affected Version(s): * Up to (including) 8.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2022	6.1	OX App Suite through 8.2 allows XSS via an attachment or OX Drive content when a client uses the len or off parameter. **CVE ID : CVE-2022-31468**	N/A	A-OPE-OX_A-051122/1715
Vendor: openbmc-project					
Product: openbmc					
Affected Version(s): From (including) 2.10.0 Up to (including) 2.13.0					
Out-of-bounds Write	27-Oct-2022	7.5	A vulnerability in bmcweb of OpenBMC Project allows user to cause denial of service. This vulnerability was identified during mitigation for CVE-2022-2809. When fuzzing the multipart_parser code using AFL++ with address sanitizer enabled to find smallest memory corruptions possible. It detected problem in how multipart_parser handles unclosed http headers. If long enough http header is passed in the multipart form without colon there is one byte overwrite on	https://github.com/openbmc/bmcweb	A-OPE-OPEN-051122/1716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			heap. It can be conducted multiple times in a loop to cause DoS. **CVE ID : CVE-2022-3409**		
Out-of-bounds Write	27-Oct-2022	7.5	A vulnerability in bmcweb of OpenBMC Project allows user to cause denial of service. When fuzzing the multipart_parser code using AFL++ with address sanitizer enabled to find smallest memory corruptions possible. It detected problem in how multipart_parser handles unclosed http headers. If long enough http header is passed in the multipart form without colon there is one byte overwrite on heap. It can be conducted multiple times in a loop to cause DoS. **CVE ID : CVE-2022-2809**	https://github.com/openbmc/bmcweb	A-OPE-OPEN-051122/1717
Vendor: opencats					
Product: opencats					
Affected Version(s): 0.9.6					
Deserialization of Untrusted Data	19-Oct-2022	9.8	OpenCATS v0.9.6 was discovered to contain a remote code execution (RCE) vulnerability via the getDataGridPager's ajax functionality. **CVE ID : CVE-2022-43019**	N/A	A-OPE-OPEN-051122/1718
Improper Neutraliz	19-Oct-2022	6.5	OpenCATS v0.9.6 was discovered to contain a	N/A	A-OPE-OPEN-051122/1719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation of Special Elements used in an SQL Command ('SQL Injection')			SQL injection vulnerability via the tag_id variable in the Tag update function. **CVE ID : CVE-2022-43020**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Oct-2022	6.5	OpenCATS v0.9.6 was discovered to contain a SQL injection vulnerability via the entriesPerPage variable. **CVE ID : CVE-2022-43021**	N/A	A-OPE-OPEN-051122/1720
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Oct-2022	6.5	OpenCATS v0.9.6 was discovered to contain a SQL injection vulnerability via the tag_id variable in the Tag deletion function. **CVE ID : CVE-2022-43022**	N/A	A-OPE-OPEN-051122/1721
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Oct-2022	6.5	OpenCATS v0.9.6 was discovered to contain a SQL injection vulnerability via the importID parameter in the Import viewerrors function. **CVE ID : CVE-2022-43023**	N/A	A-OPE-OPEN-051122/1722
Improper Neutralization of Input During	19-Oct-2022	6.1	OpenCATS v0.9.6 was discovered to contain a reflected cross-site scripting (XSS)	N/A	A-OPE-OPEN-051122/1723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			vulnerability via the joborderID parameter. **CVE ID : CVE-2022-43014**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2022	6.1	OpenCATS v0.9.6 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the entriesPerPage parameter. **CVE ID : CVE-2022-43015**	N/A	A-OPE-OPEN-051122/1724
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2022	6.1	OpenCATS v0.9.6 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the callback component. **CVE ID : CVE-2022-43016**	N/A	A-OPE-OPEN-051122/1725
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2022	6.1	OpenCATS v0.9.6 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the indexFile component. **CVE ID : CVE-2022-43017**	N/A	A-OPE-OPEN-051122/1726
Improper Neutralization of Input	19-Oct-2022	6.1	OpenCATS v0.9.6 was discovered to contain a reflected cross-site scripting (XSS)	N/A	A-OPE-OPEN-051122/1727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			vulnerability via the email parameter in the Check Email function. **CVE ID : CVE-2022-43018**		
Vendor: opencrx					
Product: opencrx					
Affected Version(s): * Up to (including) 5.2.2					
Observable Discrepancy	20-Oct-2022	5.3	OpenCRX before v5.2.2 was discovered to be vulnerable to password enumeration due to the difference in error messages received during a password reset which could enable an attacker to determine if a username, email or ID is valid. **CVE ID : CVE-2022-40084**	N/A	A-OPE-OPEN-051122/1728
Vendor: openfga					
Product: openfga					
Affected Version(s): * Up to (excluding) 0.2.4					
Incorrect Authorization	25-Oct-2022	9.8	OpenFGA is an authorization/permission engine. Versions prior to version 0.2.4 are vulnerable to authorization bypass under certain conditions. Users who have wildcard (`*`) defined on tupleset relations in their authorization model are vulnerable. Version 0.2.4 contains a patch for this issue.	https://github.com/openfga/openfga/security/advisories/GHSA-vj4m-83m8-xpw5, https://github.com/openfga/openfga/commit/b466769cc100b2065047786578718d313f52695b	A-OPE-OPEN-051122/1729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39341		
Incorrect Authorization	25-Oct-2022	9.8	OpenFGA is an authorization/permission engine. Versions prior to version 0.2.4 are vulnerable to authorization bypass under certain conditions. Users whose model has a relation defined as a tupleset (the right hand side of a â€˜fromâ€™ statement) that involves anything other than a direct relationship (e.g. â€˜as selfâ€™) are vulnerable. Version 0.2.4 contains a patch for this issue. **CVE ID : CVE-2022-39342**	https://github.com/openfga/openfga/security/advisories/GHSA-f4mm-2r69-mg5f, https://github.com/openfga/openfga/commit/c8db1ee3d2a366f18e585dd33236340e76e784c4	A-OPE-OPEN-051122/1730
Incorrect Authorization	25-Oct-2022	5.3	OpenFGA is an authorization/permission engine. Prior to version 0.2.4, the `streamed-list-objects` endpoint was not validating the authorization header, resulting in disclosure of objects in the store. Users `openfga/openfga` versions 0.2.3 and prior who are exposing the OpenFGA service to the internet are vulnerable. Version 0.2.4 contains a patch for this issue. **CVE ID : CVE-2022-39340**	https://github.com/openfga/openfga/security/advisories/GHSA-95x7-mh78-7w2r, https://github.com/openfga/openfga/commit/779d73d4b6d067ee042ec9b59fec707eed71e42f	A-OPE-OPEN-051122/1731
Vendor: opensecurity					
Product: mobile_security_framework					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 0.9.2					
N/A	18-Oct-2022	7.5	Mobile Security Framework (MobSF) v0.9.2 and below was discovered to contain a local file inclusion (LFI) vulnerability in the StaticAnalyzer/views.py script. This vulnerability allows attackers to read arbitrary files via a crafted HTTP request. **CVE ID : CVE-2022-41547**	https://github.com/MobSF/Mobile-Security-Framework-MobSF/commit/b9cdd1f52bdf127cf33bb1be369e374a2855f8e6#diff-69d2e38f6bba208c333da6a09a83ca65056fcb60f4e10d23f67c01bcc1ffb58c	A-OPE-MOBI-051122/1732
Vendor: Opensuse					
Product: factory					
Affected Version(s): * Up to (excluding) 8.17.1-1.1					
Improper Link Resolution Before File Access ('Link Following')	26-Oct-2022	7.8	A Improper Link Resolution Before File Access ('Link Following') vulnerability in a script called by the sendmail systemd service of openSUSE Factory allows local attackers to escalate from user mail to root. This issue affects: SUSE openSUSE Factory sendmail versions prior to 8.17.1-1.1. **CVE ID : CVE-2022-31256**	https://bugzilla.suse.com/show_bug.cgi?id=1204696	A-OPE-FACT-051122/1733
Vendor: opensvc					
Product: multipath-tools					
Affected Version(s): From (including) 0.7.0 Up to (excluding) 0.9.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	29-Oct-2022	0	multipath-tools 0.7.0 through 0.9.x before 0.9.2 allows local users to obtain root access, as exploited alone or in conjunction with CVE-2022-41973. Local users able to write to UNIX domain sockets can bypass access controls and manipulate the multipath setup. This can lead to local privilege escalation to root. This occurs because an attacker can repeat a keyword, which is mishandled because arithmetic ADD is used instead of bitwise OR. **CVE ID : CVE-2022-41974**	N/A	A-OPE-MULT-051122/1734
Affected Version(s): From (including) 0.7.7 Up to (excluding) 0.9.2					
N/A	29-Oct-2022	0	multipath-tools 0.7.7 through 0.9.x before 0.9.2 allows local users to obtain root access, as exploited in conjunction with CVE-2022-41974. Local users able to access /dev/shm can change symlinks in multipathd due to incorrect symlink handling, which could lead to controlled file writes outside of the /dev/shm directory. This could be used indirectly for local privilege escalation to root. **CVE ID : CVE-2022-41973**	N/A	A-OPE-MULT-051122/1735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: open_source_sacco_management_system_project					
Product: open_source_sacco_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Oct-2022	7.2	Open Source SACCO Management System v1.0 is vulnerable to SQL Injection via /sacco_shield/manage_payment.php. **CVE ID : CVE-2022-42143**	N/A	A-OPE-OPEN-051122/1736
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Oct-2022	7.2	Open Source SACCO Management System v1.0 vulnerable to SQL Injection via /sacco_shield/manage_loan.php. **CVE ID : CVE-2022-42218**	N/A	A-OPE-OPEN-051122/1737
Vendor: Oracle					
Product: access_manager					
Affected Version(s): 12.2.1.3.0					
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Authentication Engine). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks of this	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-ACCE-051122/1738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized update, insert or delete access to some of Oracle Access Manager accessible data. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-39405**		
Affected Version(s): 12.2.1.4.0					
N/A	18-Oct-2022	7.5	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Admin Console). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Access Manager accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-39412**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-ACCE-051122/1739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: applications_framework					
Affected Version(s): From (including) 12.2.6 Up to (including) 12.2.11					
N/A	18-Oct-2022	6.5	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Session Management). Supported versions that are affected are 12.2.6-12.2.11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Applications Framework accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21636**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-APPL-051122/1740
Product: bi_publisher					
Affected Version(s): 12.2.1.3.0					
N/A	18-Oct-2022	7.6	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Core Formatting API). Supported versions that are affected are 5.9.0.0, 6.4.0.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-BI_P-051122/1741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L). **CVE ID : CVE-2022-21590**		
Affected Version(s): 12.2.1.4.0					
N/A	18-Oct-2022	7.6	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Core Formatting API). Supported versions that are affected are 5.9.0.0, 6.4.0.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-BI_P-051122/1742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L). **CVE ID : CVE-2022-21590**		
Affected Version(s): 5.9.0.0.0					
N/A	18-Oct-2022	7.6	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Core Formatting API). Supported versions that are affected are 5.9.0.0, 6.4.0.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-BI_P-051122/1743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L). **CVE ID : CVE-2022-21590**		
Affected Version(s): 6.4.0.0.0					
N/A	18-Oct-2022	7.6	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Core Formatting API). Supported versions that are affected are 5.9.0.0, 6.4.0.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-BI_P-051122/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L). **CVE ID : CVE-2022-21590**		
Product: business_intelligence					
Affected Version(s): 5.9.0.0.0					
N/A	18-Oct-2022	5.7	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Server). The supported version that is affected is 5.9.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-BUSI-051122/1745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21609**		
Product: communications_billing_and_revenue_management					
Affected Version(s): From (including) 12.0.0.4.0 Up to (including) 12.0.0.7.0					
N/A	18-Oct-2022	6.5	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). Supported versions that are affected are 12.0.0.4.0-12.0.0.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Communications Billing and Revenue Management accessible	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-COMM-051122/1746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21601**		
Product: database					
Affected Version(s): 19c					
N/A	18-Oct-2022	7.2	Vulnerability in the Oracle Database - Advanced Queuing component of Oracle Database Server. The supported version that is affected is 19c. Easily exploitable vulnerability allows high privileged attacker having DBA user privilege with network access via Oracle Net to compromise Oracle Database - Advanced Queuing. Successful attacks of this vulnerability can result in takeover of Oracle Database - Advanced Queuing. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-DATA-051122/1747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21596**		
Product: database_-_sharding					
Affected Version(s): 19c					
N/A	18-Oct-2022	7.2	Vulnerability in the Oracle Database - Sharding component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows high privileged attacker having Local Logon privilege with network access via Local Logon to compromise Oracle Database - Sharding. Successful attacks of this vulnerability can result in takeover of Oracle Database - Sharding. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21603**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-DATA-051122/1748
Affected Version(s): 21c					
N/A	18-Oct-2022	7.2	Vulnerability in the Oracle Database - Sharding component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows high	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-DATA-051122/1749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker having Local Logon privilege with network access via Local Logon to compromise Oracle Database - Sharding. Successful attacks of this vulnerability can result in takeover of Oracle Database - Sharding. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21603**		
Product: database_server					
Affected Version(s): 19c					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	Vulnerability in the Oracle Services for Microsoft Transaction Server component of Oracle Database Server. The supported version that is affected is 19c. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Services for Microsoft Transaction Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Services for Microsoft Transaction Server,	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-DATA-051122/1750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Services for Microsoft Transaction Server accessible data as well as unauthorized read access to a subset of Oracle Services for Microsoft Transaction Server accessible data. Note: This vulnerability applies to Windows systems only. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21606**		
Product: e-business_suite					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.11					
N/A	18-Oct-2022	9.8	Vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-Business Suite (component: Upload). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Web	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-E-BU-051122/1751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Applications Desktop Integrator. Successful attacks of this vulnerability can result in takeover of Oracle Web Applications Desktop Integrator. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21587**		
Product: enterprise_data_quality					
Affected Version(s): 12.2.1.3.0					
N/A	18-Oct-2022	8.8	Vulnerability in the Oracle Enterprise Data Quality product of Oracle Fusion Middleware (component: Dashboard). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Data Quality. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Data Quality, attacks may significantly impact additional products (scope change).	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-ENTE-051122/1752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Data Quality accessible data as well as unauthorized update, insert or delete access to some of Oracle Enterprise Data Quality accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Data Quality. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:L). **CVE ID : CVE-2022-21613**		
N/A	18-Oct-2022	8.1	Vulnerability in the Oracle Enterprise Data Quality product of Oracle Fusion Middleware (component: Dashboard). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Data Quality. Successful attacks of this vulnerability can result	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-ENTE-051122/1753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Data Quality accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Data Quality accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2022-21612**		
N/A	18-Oct-2022	7.5	Vulnerability in the Oracle Enterprise Data Quality product of Oracle Fusion Middleware (component: Dashboard). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Data Quality. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Data Quality accessible data. CVSS 3.1 Base Score 7.5	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-ENTE-051122/1754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21614**		
N/A	18-Oct-2022	7.4	Vulnerability in the Oracle Enterprise Data Quality product of Oracle Fusion Middleware (component: Dashboard). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Data Quality. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Data Quality, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Data Quality accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-ENTE-051122/1755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R:N/UI:R/S:C/C:H/I:N/A:N). **CVE ID : CVE-2022-21615**		
Affected Version(s): 12.2.1.4.0					
N/A	18-Oct-2022	8.8	Vulnerability in the Oracle Enterprise Data Quality product of Oracle Fusion Middleware (component: Dashboard). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Data Quality. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Data Quality, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Data Quality accessible data as well as unauthorized update, insert or delete access to some of Oracle Enterprise Data Quality accessible data and unauthorized ability to	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-ENTE-051122/1756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a partial denial of service (partial DOS) of Oracle Enterprise Data Quality. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:L). **CVE ID : CVE-2022-21613**		
N/A	18-Oct-2022	8.1	Vulnerability in the Oracle Enterprise Data Quality product of Oracle Fusion Middleware (component: Dashboard). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Data Quality. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Data Quality accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Data Quality accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-ENTE-051122/1757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2022-21612**		
N/A	18-Oct-2022	7.5	Vulnerability in the Oracle Enterprise Data Quality product of Oracle Fusion Middleware (component: Dashboard). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Data Quality. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Data Quality accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21614**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-ENTE-051122/1758
N/A	18-Oct-2022	7.4	Vulnerability in the Oracle Enterprise Data Quality product of Oracle Fusion Middleware (component: Dashboard). Supported	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-ENTE-051122/1759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Data Quality. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Data Quality, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Data Quality accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N). **CVE ID : CVE-2022-21615**		
Product: enterprise_manager_base_platform					
Affected Version(s): 13.4.0.0					
N/A	18-Oct-2022	7.5	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Application Config Console). Supported	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-ENTE-051122/1760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 13.4.0.0 and 13.5.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Enterprise Manager Base Platform accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2022-21623**		
Affected Version(s): 13.5.0.0					
N/A	18-Oct-2022	7.5	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Application Config Console). Supported versions that are affected are 13.4.0.0 and 13.5.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks of this vulnerability can result	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-ENTE-051122/1761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in unauthorized creation, deletion or modification access to critical data or all Enterprise Manager Base Platform accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2022-21623**		
Product: graalvm					
Affected Version(s): 20.3.7					
N/A	18-Oct-2022	7.5	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: LLVM Interpreter). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle GraalVM Enterprise Edition. CVSS 3.1 Base Score 7.5 (Availability impacts).	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-GRAA-051122/1762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21634**		
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaScript). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GraalVM Enterprise Edition accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21597**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-GRAA-051122/1763
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component:	https://www.oracle.com/security-alerts/cpuoct2022.html,	A-ORA-GRAA-051122/1764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector:	https://security.netapp.com/advisory/ntap-20221028-0012/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21626**		
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-GRAA-051122/1765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21628**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update,	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-GRAA-051122/1766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21619**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition:	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-GRAA-051122/1767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21624**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-GRAA-051122/1768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-39399**		
Affected Version(s): 21.3.3					
N/A	18-Oct-2022	7.5	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: LLVM Interpreter). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle GraalVM Enterprise Edition. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-GRAA-051122/1769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21634		
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaScript). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GraalVM Enterprise Edition accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21597**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-GRAA-051122/1770
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JGSS). Supported versions that are affected are Oracle Java SE: 17.0.4.1, 19; Oracle	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-	A-ORA-GRAA-051122/1771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition: 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	20221028-0012/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21618		
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-GRAA-051122/1772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21626**		
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-GRAA-051122/1773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21628**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-GRAA-051122/1774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21619**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component:	https://www.oracle.com/security-alerts/cpuoct2022.html,	A-ORA-GRAA-051122/1775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JNDI). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS	https://security.netapp.com/advisory/ntap-20221028-0012/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21624**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-GRAA-051122/1776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-39399**		
Affected Version(s): 22.2.0					
N/A	18-Oct-2022	7.5	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: LLVM Interpreter). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle GraalVM	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-GRAA-051122/1777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21634**		
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaScript). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GraalVM Enterprise Edition accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21597**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-GRAA-051122/1778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JGSS). Supported versions that are affected are Oracle Java SE: 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-GRAA-051122/1779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21618**		
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets,	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-GRAA-051122/1780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21626**		
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-GRAA-051122/1781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21628**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf,	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-	A-ORA-GRAA-051122/1782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	20221028-0012/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21619		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-GRAA-051122/1783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21624**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments,	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-GRAA-051122/1784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-39399**		
Product: http_server					
Affected Version(s): 12.2.1.3.0					
N/A	18-Oct-2022	7.1	Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: OHS Config MBeans). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server. Successful attacks require human interaction from a	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-HTTP-051122/1785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle HTTP Server accessible data as well as unauthorized update, insert or delete access to some of Oracle HTTP Server accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N). **CVE ID : CVE-2022-21593**		
Affected Version(s): 12.2.1.4.0					
N/A	18-Oct-2022	7.1	Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: OHS Config MBeans). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-HTTP-051122/1786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in unauthorized access to critical data or complete access to all Oracle HTTP Server accessible data as well as unauthorized update, insert or delete access to some of Oracle HTTP Server accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N). **CVE ID : CVE-2022-21593**		
Product: java_virtual_machine					
Affected Version(s): 19c					
N/A	18-Oct-2022	4.3	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java VM accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-JAVA-051122/1787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39419		
Affected Version(s): 21c					
N/A	18-Oct-2022	4.3	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java VM accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-39419**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-JAVA-051122/1788
Product: jdk					
Affected Version(s): 1.8.0					
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21626**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21628**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21619**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21624**		
Affected Version(s): 11.0.16.1					
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component:	https://www.oracle.com/security-alerts/cpuoct2022.html,	A-ORA-JDK-051122/1793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector:	https://security.netapp.com/advisory/ntap-20221028-0012/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21626**		
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21628**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update,	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21619**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition:	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21624**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-39399**		
Affected Version(s): 17.0.4.1					
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JGSS). Supported versions that are affected are Oracle Java SE: 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21618**		
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21628**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE:	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory	A-ORA-JDK-051122/1800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/P	/ntap-20221028-0012/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21619**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21624**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-39399**		
Affected Version(s): 19					
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JGSS). Supported versions that are affected are Oracle Java SE: 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Kerberos to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21618**		
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component:	https://www.oracle.com/security-alerts/cpuoct2022.html,	A-ORA-JDK-051122/1804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Lightweight HTTP Server). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1	https://security.netapp.com/advisory/ntap-20221028-0012/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21628**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets,	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21619**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21624**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition:	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JDK-051122/1807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-39399**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: jd_edwards_enterpriseone_tools					
Affected Version(s): * Up to (including) 9.2.6.4					
N/A	18-Oct-2022	6.1	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime SEC). Supported versions that are affected are 9.2.6.4 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-JD_E-051122/1808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21630**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Design Tools SEC). Supported versions that are affected are 9.2.6.4 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-JD_E-051122/1809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21631**		
N/A	18-Oct-2022	5.4	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime SEC). Supported versions that are affected are 9.2.6.4 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 5.4	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-JD_E-051122/1810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21629**		
Product: jre					
Affected Version(s): 1.8.0					
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21626**		
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21628**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE:	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory	A-ORA-JRE-051122/1813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/P	/ntap-20221028-0012/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21619**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21624**		
Affected Version(s): 11.0.16.1					
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21626**		
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21628**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21619**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21624**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-39399**		
Affected Version(s): 17.0.4.1					
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JGSS). Supported versions that are affected are Oracle Java SE:	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory	A-ORA-JRE-051122/1820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	/ntap-20221028-0012/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21618		
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21628**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21619**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21624**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle	https://www.oracle.com/security-alerts/cpuoc	A-ORA-JRE-051122/1824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity	t2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-39399**		
Affected Version(s): 19					
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JGSS). Supported versions that are affected are Oracle Java SE: 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21618**		
N/A	18-Oct-2022	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21628**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition:	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21619**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21624**		
N/A	18-Oct-2022	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0012/	A-ORA-JRE-051122/1829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-39399**		
Product: mysql					
Affected Version(s): * Up to (including) 1.6.3					
N/A	18-Oct-2022	4.2	Vulnerability in the MySQL Installer product of Oracle MySQL (component: Installer: General). Supported versions that are affected are 1.6.3 and prior. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Installer executes to compromise MySQL Installer. Successful attacks require human interaction from a person other than the attacker. Successful	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-MYSQ-051122/1830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Installer accessible data as well as unauthorized read access to a subset of MySQL Installer accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Installer. CVSS 3.1 Base Score 4.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L). **CVE ID : CVE-2022-39404**		
Affected Version(s): From (including) 5.7.0 Up to (including) 5.7.36					
N/A	18-Oct-2022	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: C API). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21595**		
Affected Version(s): From (including) 5.7.0 Up to (including) 5.7.39					
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.39 and prior and 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21608**	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1832
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server:	https://www.oracle.com/security-alerts/cpuoc	A-ORA-MYSQ-051122/1833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connection Handling). Supported versions that are affected are 5.7.39 and prior and 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21617**	t2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	
N/A	18-Oct-2022	4.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.39 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21589**		
N/A	18-Oct-2022	4.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.7.39 and prior and 8.0.29 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21592**	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1835
Affected Version(s): From (including) 8.0 Up to (including) 8.0.16					
N/A	18-Oct-2022	4.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges).	https://www.oracle.com/security-alerts/cpuoct2022.html,	A-ORA-MYSQ-051122/1836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are 5.7.39 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21589**	https://security.netapp.com/advisory/ntap-20221028-0013/	
Affected Version(s): From (including) 8.0 Up to (including) 8.0.27					
N/A	18-Oct-2022	7.2	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts).	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21600**		
N/A	18-Oct-2022	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: C API). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21595**	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1838
Affected Version(s): From (including) 8.0 Up to (including) 8.0.28					
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Data Dictionary). Supported versions that are affected are 8.0.28	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.c	A-ORA-MYSQ-051122/1839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21605**	om/advisory/ntap-20221028-0013/	
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21607**		
Affected Version(s): From (including) 8.0 Up to (including) 8.0.29					
N/A	18-Oct-2022	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H). **CVE ID : CVE-2022-21635**	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21638**	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1842
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21641**		
N/A	18-Oct-2022	4.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.7.39 and prior and 8.0.29 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21592**	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1844
Affected Version(s): From (including) 8.0 Up to (including) 8.0.30					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-39408**	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1845
N/A	18-Oct-2022	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-39410**		
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21594**	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21599**	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1848
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21604**		
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.39 and prior and 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21608**	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are 5.7.39 and prior and 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21617**	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1851
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21632**		
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21633**	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21637**	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1854
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21640**		
N/A	18-Oct-2022	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-39400**	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21625**	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1857
N/A	18-Oct-2022	4.3	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell: Core Client). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Shell executes to compromise MySQL Shell. While the	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-MYSQ-051122/1858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is in MySQL Shell, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Shell accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2022-39402**		
N/A	18-Oct-2022	4.1	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.30 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/P	https://www.oracle.com/security-alerts/cpuoct2022.html, https://security.netapp.com/advisory/ntap-20221028-0013/	A-ORA-MYSQ-051122/1859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21611**		
N/A	18-Oct-2022	3.9	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell: Core Client). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Shell executes to compromise MySQL Shell. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Shell accessible data as well as unauthorized read access to a subset of MySQL Shell accessible data. CVSS 3.1 Base Score 3.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2022-39403**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-MYSQ-051122/1860
Product: peoplesoft_enterprise					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 8.58					
N/A	18-Oct-2022	5.3	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21602**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-PEOP-051122/1861
Affected Version(s): 8.59					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Elastic Search Integration). Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-PEOP-051122/1862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21639**		
N/A	18-Oct-2022	5.3	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-PEOP-051122/1863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21602**		
Affected Version(s): 8.60					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Elastic Search Integration). Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change).	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-PEOP-051122/1864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21639**		
N/A	18-Oct-2022	5.3	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-PEOP-051122/1865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21602**		
Product: peoplesoft_enterprise_common_components					
Affected Version(s): 9.2					
N/A	18-Oct-2022	8.1	Vulnerability in the PeopleSoft Enterprise Common Components product of Oracle PeopleSoft (component: Approval Framework). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise Common Components. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise Common Components accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise Common Components accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-PEOP-051122/1866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39406		
Product: peoplesoft_enterprise_peopletools					
Affected Version(s): 8.58					
N/A	18-Oct-2022	5.5	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Security). Supported versions that are affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where PeopleSoft Enterprise PeopleTools executes to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-39407**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-PEOP-051122/1867
Affected Version(s): 8.59					
N/A	18-Oct-2022	5.5	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Security). Supported versions that	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-PEOP-051122/1868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where PeopleSoft Enterprise PeopleTools executes to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-39407**		
Affected Version(s): 8.60					
N/A	18-Oct-2022	5.5	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Security). Supported versions that are affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where PeopleSoft Enterprise PeopleTools executes to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-PEOP-051122/1869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-39407**		
Product: siebel_core_-_db_deployment_and_configuration_accessible_data					
Affected Version(s): * Up to (including) 22.8					
N/A	18-Oct-2022	7.5	Vulnerability in the Siebel Core - DB Deployment and Configuration product of Oracle Siebel CRM (component: Repository Utilities). Supported versions that are affected are 22.8 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Core - DB Deployment and Configuration. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel Core - DB Deployment and Configuration accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-SIEB-051122/1870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2022-21598**		
Product: soa_suite					
Affected Version(s): 12.2.1.3.0					
N/A	18-Oct-2022	7.5	Vulnerability in the Oracle SOA Suite product of Oracle Fusion Middleware (component: Adapters). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle SOA Suite. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle SOA Suite accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2022-21622**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-SOA_-051122/1871
Affected Version(s): 12.2.1.4.0					
N/A	18-Oct-2022	7.5	Vulnerability in the Oracle SOA Suite product of Oracle Fusion Middleware (component: Adapters). Supported versions that are affected	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-SOA_-051122/1872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle SOA Suite. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle SOA Suite accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2022-21622**		
Product: transportation_management					
Affected Version(s): 6.5.1					
N/A	18-Oct-2022	5.4	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: UI Infrastructure). Supported versions that are affected are 6.4.3 and 6.5.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-TRAN-051122/1873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			some of Oracle Transportation Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Transportation Management. CVSS 3.1 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2022-21591**		
N/A	18-Oct-2022	5.4	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: Data, Functional Security). Supported versions that are affected are 6.4.3 and 6.5.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Transportation Management accessible data as well as unauthorized read access to a subset of Oracle Transportation	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-TRAN-051122/1874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2022-39420**		
N/A	18-Oct-2022	4.9	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: Business Process Automation). Supported versions that are affected are 6.4.3 and 6.5.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Transportation Management accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-39411**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-TRAN-051122/1875
N/A	18-Oct-2022	2.7	Vulnerability in the Oracle Transportation Management product of	https://www.oracle.com/security-	A-ORA-TRAN-051122/1876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Supply Chain (component: Business Process Automation). Supported versions that are affected are 6.4.3 and 6.5.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Transportation Management. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-39409**	alerts/cpuoct2022.html	
Affected Version(s): 6.4.3					
N/A	18-Oct-2022	5.4	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: UI Infrastructure). Supported versions that are affected are 6.4.3 and 6.5.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-TRAN-051122/1877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Transportation Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Transportation Management. CVSS 3.1 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2022-21591**		
N/A	18-Oct-2022	5.4	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: Data, Functional Security). Supported versions that are affected are 6.4.3 and 6.5.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Transportation Management accessible	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-TRAN-051122/1878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data as well as unauthorized read access to a subset of Oracle Transportation Management accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2022-39420**		
N/A	18-Oct-2022	4.9	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: Business Process Automation). Supported versions that are affected are 6.4.3 and 6.5.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Transportation Management accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-TRAN-051122/1879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39411		
N/A	18-Oct-2022	2.7	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: Business Process Automation). Supported versions that are affected are 6.4.3 and 6.5.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Transportation Management. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-39409**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-TRAN-051122/1880
Product: vm_virtualbox					
Affected Version(s): * Up to (excluding) 6.1.38					
N/A	18-Oct-2022	7.5	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.38. Difficult to exploit	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-VM_V-051122/1881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2022-39422**		
N/A	18-Oct-2022	6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.38. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-VM_V-051122/1882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2022-39423**		
Affected Version(s): * Up to (excluding) 6.1.40					
N/A	18-Oct-2022	8.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. Note: This vulnerability applies to Windows systems only.	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-VM_V-051122/1883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2022-39427**		
N/A	18-Oct-2022	8.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Difficult to exploit vulnerability allows unauthenticated attacker with network access via VRDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-39424**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-VM_V-051122/1884
N/A	18-Oct-2022	8.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Difficult to exploit	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-VM_V-051122/1885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via VRDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-39425**		
N/A	18-Oct-2022	8.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Difficult to exploit vulnerability allows unauthenticated attacker with network access via VRDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-VM_V-051122/1886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39426		
N/A	18-Oct-2022	7.5	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2022-21620**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-VM_V-051122/1887
N/A	18-Oct-2022	7.3	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Easily exploitable	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-VM_V-051122/1888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. Note: This vulnerability applies to Windows systems only. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-39421**		
N/A	18-Oct-2022	6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-VM_V-051122/1889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2022-21621**		
N/A	18-Oct-2022	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.40. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts).	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-VM_V-051122/1890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21627**		
Product: weblogic_server					
Affected Version(s): 12.2.1.3.0					
N/A	18-Oct-2022	5.2	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle WebLogic Server executes to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server as well as unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data and unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.2 (Confidentiality, Integrity and Availability impacts).	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-WEBL-051122/1891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:H). **CVE ID : CVE-2022-21616**		
Affected Version(s): 12.2.1.4.0					
N/A	18-Oct-2022	5.2	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle WebLogic Server executes to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server as well as unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data and unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-WEBL-051122/1892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:H). **CVE ID : CVE-2022-21616**		
Affected Version(s): 14.1.1.0.0					
N/A	18-Oct-2022	5.2	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle WebLogic Server executes to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server as well as unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data and unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/P	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-WEBL-051122/1893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R:H/UI:N/S:U/C:L/I:L/A:H). **CVE ID : CVE-2022-21616**		
Product: web_applications_desktop_integrator					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.11					
N/A	18-Oct-2022	9.8	Vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-Business Suite (component: Upload). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Web Applications Desktop Integrator. Successful attacks of this vulnerability can result in takeover of Oracle Web Applications Desktop Integrator. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-39428**	https://www.oracle.com/security-alerts/cpuoct2022.html	A-ORA-WEB_-051122/1894
Vendor: oroinc					
Product: orocommerce					
Affected Version(s): From (including) 4.1.0 Up to (including) 4.1.17					
Improper Neutraliz	18-Oct-2022	5.4	OroCommerce is an open-source Business to	https://github.com/oroi	A-ORO-OROC-051122/1895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation of Input During Web Page Generation ('Cross-site Scripting')			Business Commerce application. Versions between 4.1.0 and 4.1.17 inclusive, 4.2.0 and 4.2.11 inclusive, and between 5.0.0 and 5.0.3 inclusive, are vulnerable to Cross-site Scripting in the UPS Surcharge field of the Shipping rule edit page. The attacker needs permission to create or edit a shipping rule. This issue has been patched in version 5.0.6. There are no known workarounds. **CVE ID : CVE-2022-31037**	nc/orocommerce/security/advisories/GHSA-4vf4-955g-vxp2	
Affected Version(s): From (including) 4.2.0 Up to (including) 4.2.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	5.4	OroCommerce is an open-source Business to Business Commerce application. Versions between 4.1.0 and 4.1.17 inclusive, 4.2.0 and 4.2.11 inclusive, and between 5.0.0 and 5.0.3 inclusive, are vulnerable to Cross-site Scripting in the UPS Surcharge field of the Shipping rule edit page. The attacker needs permission to create or edit a shipping rule. This issue has been patched in version 5.0.6. There are no known workarounds. **CVE ID : CVE-2022-31037**	https://github.com/oroinc/orocommerce/security/advisories/GHSA-4vf4-955g-vxp2	A-ORO-OROC-051122/1896
Affected Version(s): From (including) 5.0.0 Up to (including) 5.0.3					
Improper Neutraliz	18-Oct-2022	5.4	OroCommerce is an open-source Business to	https://github.com/oroi	A-ORO-OROC-051122/1897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation of Input During Web Page Generation ('Cross-site Scripting')			Business Commerce application. Versions between 4.1.0 and 4.1.17 inclusive, 4.2.0 and 4.2.11 inclusive, and between 5.0.0 and 5.0.3 inclusive, are vulnerable to Cross-site Scripting in the UPS Surcharge field of the Shipping rule edit page. The attacker needs permission to create or edit a shipping rule. This issue has been patched in version 5.0.6. There are no known workarounds. **CVE ID : CVE-2022-31037**	nc/orocommerce/security/advisories/GHSA-4vf4-955g-vxp2	
Vendor: osgeo					
Product: shapelib					
Affected Version(s): * Up to (including) 1.5.0					
Double Free	17-Oct-2022	9.8	A double-free condition exists in contrib/shpsort.c of shapelib 1.5.0 and older releases. This issue may allow an attacker to cause a denial of service or have other unspecified impact via control over malloc. **CVE ID : CVE-2022-0699**	https://github.com/OSGeo/shapelib/commit/c75b9281a5b9452d92e1682bdfe6019a13ed819f	A-OSG-SHAP-051122/1898
Vendor: Otrs					
Product: otrs					
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.32					
Loop with Unreachable Exit Condition	17-Oct-2022	6.5	An external attacker is able to send a specially crafted email (with many recipients) and trigger a	https://otrs.com/release-notes/otrs-security-	A-OTR-OTRS-051122/1899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			potential DoS of the system **CVE ID : CVE-2022-39052**	advisory-2022-13/	
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.39					
Loop with Unreachable Exit Condition ('Infinite Loop')	17-Oct-2022	6.5	An external attacker is able to send a specially crafted email (with many recipients) and trigger a potential DoS of the system **CVE ID : CVE-2022-39052**	https://otrs.com/release-notes/otrs-security-advisory-2022-13/	A-OTR-OTRS-051122/1900
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.0.26					
Missing Authorization	17-Oct-2022	7.5	Article template contents with sensitive data could be accessed from agents without permissions. **CVE ID : CVE-2022-3501**	https://otrs.com/release-notes/otrs-security-advisory-2022-14/	A-OTR-OTRS-051122/1901
Loop with Unreachable Exit Condition ('Infinite Loop')	17-Oct-2022	6.5	An external attacker is able to send a specially crafted email (with many recipients) and trigger a potential DoS of the system **CVE ID : CVE-2022-39052**	https://otrs.com/release-notes/otrs-security-advisory-2022-13/	A-OTR-OTRS-051122/1902
Vendor: Owasp					
Product: dependency-track					
Affected Version(s): * Up to (excluding) 4.6.0					
Cleartext Storage of Sensitive Information	25-Oct-2022	4.4	Dependency-Track is a Component Analysis platform that allows organizations to identify and reduce risk in the software supply chain. Prior to version 4.6.0, performing an API request using a valid API	https://github.com/DependencyTrack/dependency-track/security/advisories/GHSA-	A-OWA-DEPE-051122/1903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key with insufficient permissions causes the API key to be written to Dependency-Track's audit log in clear text. Actors with access to the audit log can exploit this flaw to gain access to valid API keys. The issue has been fixed in Dependency-Track 4.6.0. Instead of logging the entire API key, only the last 4 characters of the key will be logged. It is strongly recommended to check historic logs for occurrences of this behavior, and re-generating API keys in case of leakage. **CVE ID : CVE-2022-39351**	gh7v-4hxp-gqp4	
Product: dependency-track_frontend					
Affected Version(s): * Up to (excluding) 4.6.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2022	5.4	@dependencytrack/frontend is a Single Page Application (SPA) used in Dependency-Track, an open source Component Analysis platform that allows organizations to identify and reduce risk in the software supply chain. Due to the common practice of providing vulnerability details in markdown format, the Dependency-Track frontend renders them using the JavaScript library Showdown. Showdown does not have	https://github.com/DependencyTrack/frontend/security/advisories/GHSA-c33w-pm52-mqvf	A-OWA-DEPE-051122/1904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			any XSS countermeasures built in, and versions before 4.6.1 of the Dependency-Track frontend did not encode or sanitize Showdown's output. This made it possible for arbitrary JavaScript included in vulnerability details via HTML attributes to be executed in context of the frontend. Actors with the `VULNERABILITY_MANAGEMENT` permission can exploit this weakness by creating or editing a custom vulnerability and providing XSS payloads in any of the following fields: Description, Details, Recommendation, or References. The payload will be executed for users with the `VIEW_PORTFOLIO` permission when browsing to the modified vulnerability's page. Alternatively, malicious JavaScript could be introduced via any of the vulnerability databases mirrored by Dependency-Track. However, this attack vector is highly unlikely, and the maintainers of Dependency-Track are not aware of any occurrence of this happening. Note that the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`Vulnerability Details` element of the `Audit Vulnerabilities` tab in the project view is not affected. The issue has been fixed in frontend version 4.6.1. **CVE ID : CVE-2022-39350**		
Vendor: oxilab					
Product: accordions					
Affected Version(s): * Up to (excluding) 2.1.0					
N/A	21-Oct-2022	7.2	Auth. WordPress Options Change (siteurl, users_can_register, default_role, admin_email and new_admin_email) vulnerability in Biplob Adhikari's Accordions – Multiple Accordions or FAQs Builder plugin (versions <= 2.0.3 on WordPress. **CVE ID : CVE-2022-38104**	https://wordpress.org/plugins/accordions-or-faqs/#developers, https://patchstack.com/database/vulnerability/accordions-or-faqs/wordpress-accordions-plugin-2-0-3-authenticated-wordpress-options-change-vulnerability?_s_id=cve	A-OXI-ACCO-051122/1905
Vendor: Paessler					
Product: prtg_network_monitor					
Affected Version(s): * Up to (excluding) 22.3.79.2108					
Improper Neutraliz	25-Oct-2022	5.3	PRTG Network Monitor through 22.2.77.2204	https://www.paessler.c	A-PAE-PRTG-051122/1906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation of Special Elements in Output Used by a Downstream Component ('Injection')			does not prevent custom input for a device's icon, which can be modified to insert arbitrary content into the style tag for that device. When the device page loads, the arbitrary Cascading Style Sheets (CSS) data is inserted into the style tag, loading malicious content. Due to PRTG Network Monitor preventing "characters, and from modern browsers disabling JavaScript support in style tags, this vulnerability could not be escalated into a Cross-Site Scripting vulnerability. **CVE ID : CVE-2022-35739**	om/prtg/history/stable	
Vendor: parseplatform					
Product: parse-server					
Affected Version(s): * Up to (excluding) 4.10.17					
Improper Input Validation	24-Oct-2022	7.5	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Versions prior to 4.10.17, and prior to 5.2.8 on the 5.x branch, crash when a file download request is received with an invalid byte range, resulting in a Denial of Service. This issue has been patched in versions 4.10.17, and 5.2.8. There are no known workarounds.	https://github.com/parse-community/parse-server/security/advisories/GHSA-h423-w6qv-2wj3	A-PAR-PARS-051122/1907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39313		
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.2.8					
Improper Input Validation	24-Oct-2022	7.5	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Versions prior to 4.10.17, and prior to 5.2.8 on the 5.x branch, crash when a file download request is received with an invalid byte range, resulting in a Denial of Service. This issue has been patched in versions 4.10.17, and 5.2.8. There are no known workarounds. **CVE ID : CVE-2022-39313**	https://github.com/parse-community/parse-server/security/advisories/GHSA-h423-w6qv-2wj3	A-PAR-PARS-051122/1908
Vendor: passster_project					
Product: passster					
Affected Version(s): * Up to (excluding) 3.5.5.5.2					
Inadequate Encryption Strength	17-Oct-2022	5.9	The Passster WordPress plugin before 3.5.5.5.2 stores the password inside a cookie named "passster" using base64 encoding method which is easy to decode. This puts the password at risk in case the cookies get leaked. **CVE ID : CVE-2022-3206**	N/A	A-PAS-PASS-051122/1909
Vendor: password_storage_application_project					
Product: password_storage_application					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2022	5.4	Password Storage Application v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the Setup page. **CVE ID : CVE-2022-42993**	N/A	A-PAS-PASS-051122/1910
Vendor: pctechsoft					
Product: pcsecure					
Affected Version(s): 5.0.8.xw					
Use of Hard-coded Credentials	20-Oct-2022	7.8	In PCTechSoft PCSecure V5.0.8.xw, use of Hard-coded Credentials in configuration files leads to admin panel access. **CVE ID : CVE-2022-42176**	N/A	A-PCT-PCSE-051122/1911
Vendor: phoenixframework					
Product: phoenix					
Affected Version(s): * Up to (excluding) 1.6.14					
N/A	17-Oct-2022	0	socket/transport.ex in Phoenix before 1.6.14 mishandles check_origin wildcarding. NOTE: LiveView applications are unaffected by default because of the presence of a LiveView CSRF token. **CVE ID : CVE-2022-42975**	N/A	A-PHO-PHOE-051122/1912
Vendor: Phpmyfaq					
Product: phpmyfaq					
Affected Version(s): * Up to (excluding) 3.1.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	29-Oct-2022	0	Weak Password Requirements in GitHub repository thorsten/phpmyfaq prior to 3.1.8. **CVE ID : CVE-2022-3754**	https://huntr.dev/bounties/f4711d7f-1368-48ab-9bef-45f32e356c47	A-PHP-PHPM-051122/1913
Affected Version(s): * Up to (including) 3.1.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2022	8.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.2.0-alpha. **CVE ID : CVE-2022-3608**	https://huntr.dev/bounties/8f0f3635-9d81-4c55-9826-2ba955c3a850, https://github.com/thorsten/phpmyfaq/commit/37123edd50f854bd141e6fbe65221af2d5cf2677	A-PHP-PHPM-051122/1914
Vendor: phpok					
Product: phpok					
Affected Version(s): 6.1					
Deserialization of Untrusted Data	18-Oct-2022	9.8	Phpok 6.1 has a deserialization vulnerability via framework/phpok_call.php. **CVE ID : CVE-2022-40889**	N/A	A-PHP-PHPO-051122/1915
Vendor: pikepdf_project					
Product: pikepdf					
Affected Version(s): * Up to (excluding) 2.10.0					
Improper Restriction of XML External	24-Oct-2022	9.8	pikepdf before 2.10.0 allows an XXE attack	https://bugs.gentoo.org/779475	A-PIK-PIKE-051122/1916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Entity Reference			against PDF XMP metadata parsing. **CVE ID : CVE-2021-46849**		
Vendor: Pimcore					
Product: pimcore					
Affected Version(s): * Up to (excluding) 10.5.9					
Improper Control of Generation of Code ('Code Injection')	27-Oct-2022	9.8	Pimcore is an open source data and experience management platform. Prior to version 10.5.9, the user controlled twig templates rendering in `Pimcore/Mail` & `ClassDefinition\Layout\Text` is vulnerable to server-side template injection, which could lead to remote code execution. Version 10.5.9 contains a patch for this issue. As a workaround, one may apply the patch manually. **CVE ID : CVE-2022-39365**	https://github.com/pimcore/pimcore/security/advisories/GHSA-5qxq-vgmm-q39m,https://github.com/pimcore/pimcore/commit/43aa34e018f5cd447bceb864358285ba92f68372	A-PIM-PIMC-051122/1917
Vendor: Pivotal					
Product: reactor_netty					
Affected Version(s): From (including) 1.0.11 Up to (including) 1.0.23					
N/A	19-Oct-2022	4.3	Reactor Netty HTTP Server, in versions 1.0.11 - 1.0.23, may log request headers in some cases of invalid HTTP requests. The logged headers may reveal valid access tokens to those with access to server logs. This may affect only invalid HTTP requests	https://tanzu.vmware.com/security/cve-2022-31684	A-PIV-REAC-051122/1918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			where logging at WARN level is enabled. **CVE ID : CVE-2022-31684**		
Vendor: Pulpproject					
Product: pulp_ansible					
Affected Version(s): -					
Insufficiently Protected Credentials	25-Oct-2022	5.5	The collection remote for pulp_ansible stores tokens in plaintext instead of using pulp's encrypted field and exposes them in read/write mode via the API () instead of marking it as write only. **CVE ID : CVE-2022-3644**	N/A	A-PUL-PULP-051122/1919
Vendor: pwndoc_project					
Product: pwndoc					
Affected Version(s): * Up to (including) 0.5.3					
N/A	30-Oct-2022	0	PwnDoc through 0.5.3 might allow remote attackers to identify disabled user account names by leveraging response timings for authentication attempts. **CVE ID : CVE-2022-44023**	N/A	A-PWN-PWND-051122/1920
N/A	30-Oct-2022	0	PwnDoc through 0.5.3 might allow remote attackers to identify valid user account names by leveraging response timings for authentication attempts. **CVE ID : CVE-2022-44022**	N/A	A-PWN-PWND-051122/1921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: pytest					
Product: py					
Affected Version(s): * Up to (including) 1.11.0					
N/A	16-Oct-2022	7.5	The py library through 1.11.0 for Python allows remote attackers to conduct a ReDoS (Regular expression Denial of Service) attack via a Subversion repository with crafted info data, because the InfoSvnCommand argument is mishandled. **CVE ID : CVE-2022-42969**	N/A	A-PYT-PY-051122/1922
Vendor: Qemu					
Product: qemu					
Affected Version(s): From (including) 6.1.0 Up to (including) 7.1.0					
Integer Underflow (Wrap or Wraparound)	17-Oct-2022	6.5	An integer underflow issue was found in the QEMU VNC server while processing ClientCutText messages in the extended format. A malicious client could use this flaw to make QEMU unresponsive by sending a specially crafted payload message, resulting in a denial of service. **CVE ID : CVE-2022-3165**	https://gitlab.com/qemu-project/qemu/-/commit/d307040b18	A-QEM-QEMU-051122/1923
Vendor: ragic					
Product: ragic					
Affected Version(s): * Up to (including) 2022-06-28					
Improper Neutraliz	31-Oct-2022	5.4	Ragic report generation page has insufficient	N/A	A-RAG-RAGI-051122/1924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation of Input During Web Page Generation ('Cross-site Scripting')			filtering for special characters. A remote attacker with general user privilege can inject JavaScript to perform XSS (Reflected Cross-Site Scripting) attack. **CVE ID : CVE-2022-40739**		
Vendor: Redhat					
Product: 3scale_api_management					
Affected Version(s): 2.0					
Improper Input Validation	19-Oct-2022	8.8	3scale API Management 2 does not perform adequate sanitation for user input in multiple fields. An authenticated user could use this flaw to inject scripts and possibly gain access to sensitive information or conduct further attacks. **CVE ID : CVE-2022-1414**	https://bugzilla.redhat.com/show_bug.cgi?id=2076794, https://access.redhat.com/security/cve/CVE-2022-1414	A-RED-3SCA-051122/1925
Product: ansible_automation_platform					
Affected Version(s): 2.0					
Insufficiently Protected Credentials	25-Oct-2022	5.5	The collection remote for pulp_ansible stores tokens in plaintext instead of using pulp's encrypted field and exposes them in read/write mode via the API () instead of marking it as write only. **CVE ID : CVE-2022-3644**	N/A	A-RED-ANSI-051122/1926
Product: satellite					
Affected Version(s): 6.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	25-Oct-2022	5.5	The collection remote for pulp_ansible stores tokens in plaintext instead of using pulp's encrypted field and exposes them in read/write mode via the API () instead of marking it as write only. **CVE ID : CVE-2022-3644**	N/A	A-RED-SATE-051122/1927
Product: update_infrastructure					
Affected Version(s): 3.0					
Insufficiently Protected Credentials	25-Oct-2022	5.5	The collection remote for pulp_ansible stores tokens in plaintext instead of using pulp's encrypted field and exposes them in read/write mode via the API () instead of marking it as write only. **CVE ID : CVE-2022-3644**	N/A	A-RED-UPDA-051122/1928
Product: virtualization					
Affected Version(s): 4.0					
Cleartext Storage of Sensitive Information	19-Oct-2022	6.5	A flaw was found in ovirt-engine, which leads to the logging of plaintext passwords in the log file when using otapi-style. This flaw allows an attacker with sufficient privileges to read the log file, leading to confidentiality loss. **CVE ID : CVE-2022-2805**	https://access.redhat.com/security/cve/CVE-2022-2805, https://bugzilla.redhat.com/show_bug.cgi?id=2079545	A-RED-VIRT-051122/1929
Vendor: redis					
Product: redis					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Uncontrolled Search Path Element	28-Oct-2022	9.8	A vulnerability was found in Redis. It has been declared as critical. This vulnerability affects unknown code in the library C:/Program Files/Redis/dbghelp.dll. The manipulation leads to uncontrolled search path. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-212416. **CVE ID : CVE-2022-3734**	N/A	A-RED-REDI-051122/1930
Affected Version(s): * Up to (excluding) 2022-09-29					
Improper Resource Shutdown or Release	21-Oct-2022	7.5	A vulnerability, which was classified as problematic, was found in Redis. Affected is the function sigsegvHandler of the file debug.c of the component Crash Report. The manipulation leads to denial of service. The name of the patch is 0bf90d944313919eb8e63d3588bf63a367f020a3. It is recommended to apply a patch to fix this issue. VDB-211962 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3647**	https://github.com/redis/redis/commit/0bf90d944313919eb8e63d3588bf63a367f020a3	A-RED-REDI-051122/1931
Vendor: relatedcode					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: messenger					
Affected Version(s): -					
N/A	19-Oct-2022	6.5	Relatedcode's Messenger version 7bcd20b allows an authenticated external attacker to access sensitive data of any user of the application. This is possible because the application exposes user data to the public. **CVE ID : CVE-2022-41707**	N/A	A-REL-MESS-051122/1932
Improper Preservation of Permissions	19-Oct-2022	4.3	Relatedcode's Messenger version 7bcd20b allows an authenticated external attacker to access existing chats in the workspaces of any user of the application. This is possible because the application does not validate permissions correctly. **CVE ID : CVE-2022-41708**	N/A	A-REL-MESS-051122/1933
Vendor: retain					
Product: retain_live_chat					
Affected Version(s): * Up to (including) 0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2022	4.8	The Retain Live Chat WordPress plugin through 0.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html	https://wpscan.com/vulnerability/ec51420-ee50-4e39-a38d-09686f1996f2	A-RET-RETA-051122/1934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-3391**		
Vendor: Rockwellautomation					
Product: factorytalk_alarms_and_events					
Affected Version(s): -					
Improper Authentication	27-Oct-2022	7.5	An unauthenticated attacker with network access to a victim's Rockwell Automation FactoryTalk Alarm and Events service could open a connection, causing the service to fault and become unavailable. The affected port could be used as a server ping port and uses messages structured with XML. **CVE ID : CVE-2022-38744**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1136876	A-ROC-FACT-051122/1935
Product: factorytalk_vantagepoint					
Affected Version(s): 8.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Oct-2022	8.8	Rockwell Automation FactoryTalk VantagePoint versions 8.0, 8.10, 8.20, 8.30, 8.31 are vulnerable to an input validation vulnerability. The FactoryTalk VantagePoint SQL Server lacks input validation when users enter SQL statements to retrieve information from the back-end database. If successfully exploited,	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137043	A-ROC-FACT-051122/1936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this could allow a user with basic user privileges to perform remote code execution on the server. **CVE ID : CVE-2022-3158**		
N/A	17-Oct-2022	8.8	Rockwell Automation FactoryTalk VantagePoint versions 8.0, 8.10, 8.20, 8.30, 8.31 are vulnerable to an improper access control vulnerability. The FactoryTalk VantagePoint SQL Server account could allow a malicious user with read-only privileges to execute SQL statements in the back-end database. If successfully exploited, this could allow the attacker to execute arbitrary code and gain access to restricted data. **CVE ID : CVE-2022-38743**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137043	A-ROC-FACT-051122/1937
Affected Version(s): 8.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Oct-2022	8.8	Rockwell Automation FactoryTalk VantagePoint versions 8.0, 8.10, 8.20, 8.30, 8.31 are vulnerable to an input validation vulnerability. The FactoryTalk VantagePoint SQL Server lacks input validation when users enter SQL statements to retrieve information from the back-end database. If	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137043	A-ROC-FACT-051122/1938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successfully exploited, this could allow a user with basic user privileges to perform remote code execution on the server. **CVE ID : CVE-2022-3158**		
N/A	17-Oct-2022	8.8	Rockwell Automation FactoryTalk VantagePoint versions 8.0, 8.10, 8.20, 8.30, 8.31 are vulnerable to an improper access control vulnerability. The FactoryTalk VantagePoint SQL Server account could allow a malicious user with read-only privileges to execute SQL statements in the back-end database. If successfully exploited, this could allow the attacker to execute arbitrary code and gain access to restricted data. **CVE ID : CVE-2022-38743**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137043	A-ROC-FACT-051122/1939
Affected Version(s): 8.20					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Oct-2022	8.8	Rockwell Automation FactoryTalk VantagePoint versions 8.0, 8.10, 8.20, 8.30, 8.31 are vulnerable to an input validation vulnerability. The FactoryTalk VantagePoint SQL Server lacks input validation when users enter SQL statements to retrieve information from the	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137043	A-ROC-FACT-051122/1940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			back-end database. If successfully exploited, this could allow a user with basic user privileges to perform remote code execution on the server. **CVE ID : CVE-2022-3158**		
N/A	17-Oct-2022	8.8	Rockwell Automation FactoryTalk VantagePoint versions 8.0, 8.10, 8.20, 8.30, 8.31 are vulnerable to an improper access control vulnerability. The FactoryTalk VantagePoint SQL Server account could allow a malicious user with read-only privileges to execute SQL statements in the back-end database. If successfully exploited, this could allow the attacker to execute arbitrary code and gain access to restricted data. **CVE ID : CVE-2022-38743**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137043	A-ROC-FACT-051122/1941
Affected Version(s): 8.30					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Oct-2022	8.8	Rockwell Automation FactoryTalk VantagePoint versions 8.0, 8.10, 8.20, 8.30, 8.31 are vulnerable to an input validation vulnerability. The FactoryTalk VantagePoint SQL Server lacks input validation when users enter SQL statements to retrieve	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137043	A-ROC-FACT-051122/1942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information from the back-end database. If successfully exploited, this could allow a user with basic user privileges to perform remote code execution on the server. **CVE ID : CVE-2022-3158**		
N/A	17-Oct-2022	8.8	Rockwell Automation FactoryTalk VantagePoint versions 8.0, 8.10, 8.20, 8.30, 8.31 are vulnerable to an improper access control vulnerability. The FactoryTalk VantagePoint SQL Server account could allow a malicious user with read-only privileges to execute SQL statements in the back-end database. If successfully exploited, this could allow the attacker to execute arbitrary code and gain access to restricted data. **CVE ID : CVE-2022-38743**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137043	A-ROC-FACT-051122/1943
Affected Version(s): 8.31					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Oct-2022	8.8	Rockwell Automation FactoryTalk VantagePoint versions 8.0, 8.10, 8.20, 8.30, 8.31 are vulnerable to an input validation vulnerability. The FactoryTalk VantagePoint SQL Server lacks input validation when users enter SQL	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137043	A-ROC-FACT-051122/1944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			statements to retrieve information from the back-end database. If successfully exploited, this could allow a user with basic user privileges to perform remote code execution on the server. **CVE ID : CVE-2022-3158**		
N/A	17-Oct-2022	8.8	Rockwell Automation FactoryTalk VantagePoint versions 8.0, 8.10, 8.20, 8.30, 8.31 are vulnerable to an improper access control vulnerability. The FactoryTalk VantagePoint SQL Server account could allow a malicious user with read-only privileges to execute SQL statements in the back-end database. If successfully exploited, this could allow the attacker to execute arbitrary code and gain access to restricted data. **CVE ID : CVE-2022-38743**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137043	A-ROC-FACT-051122/1945
Vendor: Rubyonrails					
Product: rails					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-	26-Oct-2022	5.4	A vulnerability classified as problematic has been found in Ruby on Rails. This affects an unknown part of the file actionpack/lib/action_dispatch/middleware/templates/routes/_table.htm	https://github.com/rails/rails/issues/46244, https://github.com/rails/rails/commit/be177e45	A-RUB-RAIL-051122/1946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
site Scripting')			l.erb. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The name of the patch is be177e4566747b73ff63fd5f529fab564e475ed4. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-212319. **CVE ID : CVE-2022-3704**	66747b73ff63fd5f529fab564e475ed4	
Vendor: rukovoditel					
Product: rukovoditel					
Affected Version(s): 3.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-2022	5.4	A stored cross-site scripting (XSS) vulnerability in the Global Lists feature (/index.php?module=global_lists/lists) of Rukovoditel v3.2.1 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter after clicking "Add". **CVE ID : CVE-2022-43164**	N/A	A-RUK-RUKO-051122/1947
Improper Neutralization of Input During Web Page Generation ('Cross-	28-Oct-2022	5.4	A stored cross-site scripting (XSS) vulnerability in the Global Variables feature (/index.php?module=global_vars/vars) of Rukovoditel v3.2.1 allows authenticated	N/A	A-RUK-RUKO-051122/1948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
site Scripting')			attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Value parameter after clicking "Create". **CVE ID : CVE-2022-43165**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-2022	5.4	A stored cross-site scripting (XSS) vulnerability in the Global Entities feature (/index.php?module=entities/entities) of Rukovoditel v3.2.1 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter after clicking "Add New Entity". **CVE ID : CVE-2022-43166**	N/A	A-RUK-RUKO-051122/1949
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2022	5.4	A stored cross-site scripting (XSS) vulnerability in the Configuration/Holidays module of Rukovoditel v3.2.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter. **CVE ID : CVE-2022-43185**	N/A	A-RUK-RUKO-051122/1950
Vendor: sanitization_management_system_project					
Product: sanitization_management_system					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	26-Oct-2022	9.8	A vulnerability has been found in SourceCodester Sanitization Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to missing authentication. The attack can be launched remotely. The identifier VDB-212017 was assigned to this vulnerability. **CVE ID : CVE-2022-3674**	N/A	A-SAN-SANI-051122/1951
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2022	6.1	A vulnerability, which was classified as problematic, has been found in SourceCodester Sanitization Management System 1.0. This issue affects some unknown processing of the file /php-sms/classes/SystemSettings.php. The manipulation of the argument name/shortname leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-212015. **CVE ID : CVE-2022-3672**	N/A	A-SAN-SANI-051122/1952
Improper Neutralization of Input	26-Oct-2022	6.1	A vulnerability, which was classified as problematic, was found in SourceCodester	N/A	A-SAN-SANI-051122/1953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Sanitization Management System 1.0. Affected is an unknown function of the file /php-sms/classes/Master.php. The manipulation of the argument message leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-212016. **CVE ID : CVE-2022-3673**		
Vendor: school_activity_updates_with_sms_notification_project					
Product: school_activity_updates_with_sms_notification					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Oct-2022	9.8	School Activity Updates with SMS Notification v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /modules/announcement/index.php?view=edit&id=. **CVE ID : CVE-2022-39976**	N/A	A-SCH-SCHO-051122/1954
Vendor: Sem-cms					
Product: Semcms					
Affected Version(s): 1.2					
Improper Neutralization of Special Elements used in an SQL Command	28-Oct-2022	9.8	SEMCMS v 1.2 is vulnerable to SQL Injection via SEMCMS_User.php. **CVE ID : CVE-2021-38217**	N/A	A-SEM-SEMC-051122/1955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')					
Affected Version(s): 1.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	9.8	SEMCMS SHOP v 1.1 is vulnerable to SQL Injection via Ant_BlogCat.php. **CVE ID : CVE-2021-38733**	https://www.sem-cms.cn/wenda/view-56.html	A-SEM-SEMC-051122/1956
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	9.8	SEMCMS SHOP v 1.1 is vulnerable to SQL via Ant_Message.php. **CVE ID : CVE-2021-38732**	https://www.sem-cms.cn/wenda/view-56.html	A-SEM-SEMC-051122/1957
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	9.8	SEMCMS SHOP v 1.1 is vulnerable to SQL Injection via Ant_Zekou.php. **CVE ID : CVE-2021-38731**	https://www.sem-cms.cn/wenda/view-56.html	A-SEM-SEMC-051122/1958
Improper Neutralization of Special Elements used in an SQL Command	28-Oct-2022	9.8	SEMCMS SHOP v 1.1 is vulnerable to SQL Injection via Ant_Info.php. **CVE ID : CVE-2021-38730**	https://www.sem-cms.cn/wenda/view-56.html	A-SEM-SEMC-051122/1959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	9.8	SEMCMS SHOP v 1.1 is vulnerable to SQL Injection via Ant_Plist.php. **CVE ID : CVE-2021-38729**	https://www.sem-cms.cn/wenda/view-56.html	A-SEM-SEMC-051122/1960
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	9.8	SEMCMS v 1.1 is vulnerable to SQL Injection via Ant_Pro.php. **CVE ID : CVE-2021-38737**	https://www.sem-cms.cn/wenda/view-56.html	A-SEM-SEMC-051122/1961
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	9.8	SEMCMS Shop V 1.1 is vulnerable to SQL Injection via Ant_Global.php. **CVE ID : CVE-2021-38736**	https://www.sem-cms.cn/wenda/view-56.html	A-SEM-SEMC-051122/1962
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	9.8	SEMCMS SHOP v 1.1 is vulnerable to SQL Injection via Ant_Menu.php. **CVE ID : CVE-2021-38734**	https://www.sem-cms.cn/wenda/view-56.html	A-SEM-SEMC-051122/1963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-2022	6.1	SEMCMS SHOP v 1.1 is vulnerable to Cross Site Scripting (XSS) via Ant_M_Coup.php. **CVE ID : CVE-2021-38728**	https://www.sem-cms.cn/wenda/view-56.html	A-SEM-SEMC-051122/1964
Vendor: shescape_project					
Product: shescape					
Affected Version(s): 1.6.0					
N/A	27-Oct-2022	7.5	The package shescape from 1.5.10 and before 1.6.1 are vulnerable to Regular Expression Denial of Service (ReDoS) via the escape function in index.js, due to the usage of insecure regex in the escapeArgBash function. **CVE ID : CVE-2022-25918**	https://github.com/ericcornelissen/shescape/commit/552e8eab56861720b1d4e5474fb65741643358f9, https://security.snyk.io/vuln/SNYK-JS-SHESCAPE-3061108	A-SHE-SHES-051122/1965
Affected Version(s): 1.5.10					
N/A	27-Oct-2022	7.5	The package shescape from 1.5.10 and before 1.6.1 are vulnerable to Regular Expression Denial of Service (ReDoS) via the escape function in index.js, due to the usage of insecure regex in the escapeArgBash function. **CVE ID : CVE-2022-25918**	https://github.com/ericcornelissen/shescape/commit/552e8eab56861720b1d4e5474fb65741643358f9, https://security.snyk.io/vuln/SNYK-	A-SHE-SHES-051122/1966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				JS-SHESCAPE-3061108	
Vendor: shinken-monitoring					
Product: shinken_monitoring					
Affected Version(s): 2.4.3					
Missing Authentication for Critical Function	20-Oct-2022	9.8	Shinken Solutions Shinken Monitoring Version 2.4.3 affected is vulnerable to Incorrect Access Control. The SafeUnpickler class found in shinken/safepickle.py implements a weak authentication scheme when unserializing objects passed from monitoring nodes to the Shinken monitoring server. **CVE ID : CVE-2022-37298**	https://github.com/dbyio/cve-2022-37298, https://github.com/naparuba/shinken/commit/2dae40fd1e713aec9e1966a0ab7a580b9180cff2	A-SHI-SHIN-051122/1967
Vendor: Siemens					
Product: jt2go					
Affected Version(s): * Up to (excluding) 13.3.0.5					
Out-of-bounds Write	20-Oct-2022	7.8	The APDFL.dll in Siemens JT2Go prior to V13.3.0.5 and Siemens Teamcenter Visualization prior to V14.0.0.2 contains an out of bounds write past the fixed-length heap-based buffer while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process.	https://cert-portal.siemens.com/productcert/pdf/ssa-829738.pdf, https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-07	A-SIE-JT2G-051122/1968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2069		
Product: siveillance_video_mobile_server					
Affected Version(s): * Up to (excluding) 22.2a\\(80\\)					
Incorrect Authorization	21-Oct-2022	9.8	A vulnerability has been identified in Siveillance Video Mobile Server V2022 R2 (All versions < V22.2a (80)). The mobile server component of affected applications improperly handles the log in for Active Directory accounts that are part of Administrators group. This could allow an unauthenticated remote attacker to access the application without a valid account. **CVE ID : CVE-2022-43400**	https://cert-portal.siemens.com/productcert/pdf/ssa-640732.pdf	A-SIE-SIVE-051122/1969
Product: teamcenter_visualization					
Affected Version(s): From (including) 13.3.0 Up to (excluding) 13.3.0.5					
Out-of-bounds Write	20-Oct-2022	7.8	The APDFL.dll in Siemens JT2Go prior to V13.3.0.5 and Siemens Teamcenter Visualization prior to V14.0.0.2 contains an out of bounds write past the fixed-length heap-based buffer while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2022-2069**	https://cert-portal.siemens.com/productcert/pdf/ssa-829738.pdf, https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-07	A-SIE-TEAM-051122/1970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 14.0 Up to (excluding) 14.0.0.2					
Out-of-bounds Write	20-Oct-2022	7.8	The APDFL.dll in Siemens JT2Go prior to V13.3.0.5 and Siemens Teamcenter Visualization prior to V14.0.0.2 contains an out of bounds write past the fixed-length heap-based buffer while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2022-2069**	https://cert-portal.siemens.com/productcert/pdf/ssa-829738.pdf, https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-07	A-SIE-TEAM-051122/1971
Vendor: simple_cold_storage_management_system_project					
Product: simple_cold_storage_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	17-Oct-2022	7.2	A vulnerability was found in SourceCodester Simple Cold Storage Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /csms/admin/?page=user/manage_user of the component Avatar Handler. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-211049 was assigned to this vulnerability.	N/A	A-SIM-SIMP-051122/1972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3549		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	5.4	A vulnerability was found in SourceCodester Simple Cold Storage Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component My Account. The manipulation of the argument First Name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-211201 was assigned to this vulnerability. **CVE ID : CVE-2022-3587**	N/A	A-SIM-SIMP-051122/1973
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	4.8	A vulnerability was found in SourceCodester Simple Cold Storage Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /csms/admin/?page=user/list of the component Create User Handler. The manipulation of the argument First Name/Last Name leads to cross site scripting. The attack may be launched remotely. The	N/A	A-SIM-SIMP-051122/1974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. VDB-211046 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3546**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	4.8	A vulnerability was found in SourceCodester Simple Cold Storage Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /csms/admin/?page=system_info of the component Setting Handler. The manipulation of the argument System Name/System Short Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-211047. **CVE ID : CVE-2022-3547**	N/A	A-SIM-SIMP-051122/1975
Improper Neutralization of Input During Web Page Generation ('Cross-site	17-Oct-2022	4.8	A vulnerability was found in SourceCodester Simple Cold Storage Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the component Add New	N/A	A-SIM-SIMP-051122/1976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			Storage Handler. The manipulation of the argument Name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-211048. **CVE ID : CVE-2022-3548**		
Cross-Site Request Forgery (CSRF)	18-Oct-2022	4.3	A vulnerability classified as problematic has been found in SourceCodester Simple Cold Storage Management System 1.0. Affected is an unknown function of the file /csms/?page=contact_us of the component Contact Us. The manipulation leads to cross-site request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-211194 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3585**	N/A	A-SIM-SIMP-051122/1977
Cross-Site Request Forgery (CSRF)	18-Oct-2022	3.5	A vulnerability has been found in SourceCodester Simple Cold Storage Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality.	N/A	A-SIM-SIMP-051122/1978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument change password leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-211189 was assigned to this vulnerability. **CVE ID : CVE-2022-3582**		
Product: simple_cold_storage_managment_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	7.2	Simple Cold Storage Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /bookings/update_status.php. **CVE ID : CVE-2022-43229**	N/A	A-SIM-SIMP-051122/1979
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	7.2	Simple Cold Storage Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/?page=bookings/view_details. **CVE ID : CVE-2022-43230**	N/A	A-SIM-SIMP-051122/1980
Vendor: simple_exam_reviewer_management_system_project					
Product: simple_exam_reviewer_management_system					
Affected Version(s): 1.0					
Unrestricted Upload	20-Oct-2022	8.8	In Simple Exam Reviewer Management System v1.0	N/A	A-SIM-SIMP-051122/1981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of File with Dangerous Type			the User List function suffers from insecure file upload. **CVE ID : CVE-2022-42198**		
Cross-Site Request Forgery (CSRF)	20-Oct-2022	8.8	Simple Exam Reviewer Management System v1.0 is vulnerable to Cross Site Request Forgery (CSRF) via the Exam List. **CVE ID : CVE-2022-42199**	N/A	A-SIM-SIMP-051122/1982
Unrestricted Upload of File with Dangerous Type	20-Oct-2022	7.2	Simple Exam Reviewer Management System v1.0 is vulnerable to Insecure file upload. **CVE ID : CVE-2022-42201**	N/A	A-SIM-SIMP-051122/1983
Improper Privilege Management	20-Oct-2022	6.5	In Simple Exam Reviewer Management System v1.0 the User List function has improper access control that allows low privileged users to modify user permissions to higher privileges. **CVE ID : CVE-2022-42197**	N/A	A-SIM-SIMP-051122/1984
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2022	5.4	Simple Exam Reviewer Management System v1.0 is vulnerable to Stored Cross Site Scripting (XSS) via the Exam List. **CVE ID : CVE-2022-42200**	N/A	A-SIM-SIMP-051122/1985
Vendor: simple_online_public_access_catalog_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: simple_online_public_access_catalog					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2022	5.4	A stored cross-site scripting (XSS) vulnerability in Simple Online Public Access Catalog v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Edit Account Full Name field. **CVE ID : CVE-2022-42991**	N/A	A-SIM-SIMP-051122/1986
Vendor: Smackcoders					
Product: an_ultimate_wordpress_importer_cum_migration_as_csv_\&_xml					
Affected Version(s): * Up to (excluding) 6.5.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Oct-2022	7.2	The Import all XML, CSV & TXT WordPress plugin before 6.5.8 does not properly sanitise and escape imported data before using them back SQL statements, leading to SQL injection exploitable by high privilege users such as admin **CVE ID : CVE-2022-3243**	N/A	A-SMA-AN_U-051122/1987
Missing Authorization	17-Oct-2022	4.2	The Import all XML, CSV & TXT WordPress plugin before 6.5.8 does not have authorisation in some places, which could allow any authenticated users to access some of the plugin features if they manage to get the related nonce	N/A	A-SMA-AN_U-051122/1988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3244		
Vendor: socket					
Product: socket.io-parser					
Affected Version(s): * Up to (excluding) 4.2.1					
N/A	26-Oct-2022	9.8	Due to improper type validation in attachment parsing the Socket.io js library, it is possible to overwrite the _placeholder object which allows an attacker to place references to functions at arbitrary places in the resulting query object. **CVE ID : CVE-2022-2421**	https://csirt.divd.nl/cves/CVE-2022-2421, https://csirt.divd.nl/cases/DIVD-2022-00045	A-SOC-SOCK-051122/1989
Vendor: soflyy					
Product: wp_all_export					
Affected Version(s): * Up to (excluding) 1.7.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2022	8.8	The WP All Export Pro WordPress plugin before 1.7.9 uses the contents of the cc_sql POST parameter directly as a database query, allowing users which has been given permission to run exports to execute arbitrary SQL statements, leading to a SQL Injection vulnerability. By default only users with the Administrator role can perform exports, but this can be delegated to lower privileged users as well.	https://wpscan.com/vulnerability/10742154-368a-40be-a67d-80ea848493a0	A-SOF-WP_A-051122/1990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3395		
Improper Control of Generation of Code ('Code Injection')	25-Oct-2022	7.2	The WP All Export Pro WordPress plugin before 1.7.9 does not limit some functionality during exports only to users with the Administrator role, allowing any logged in user which has been given privileges to perform exports to execute arbitrary code on the site. By default only administrators can run exports, but the privilege can be delegated to lower privileged users. **CVE ID : CVE-2022-3394**	https://wpscan.com/vulnerability/3266eb59-a8b2-4a5a-ab48-01a9af631b2c	A-SOF-WP_A-051122/1991
Vendor: Softing					
Product: edgeaggregator					
Affected Version(s): * Up to (including) 3.50					
Out-of-bounds Write	20-Oct-2022	7.5	An issue was discovered in Softing OPC UA C++ SDK before 6.10. A buffer overflow or an excess allocation happens due to unchecked array and matrix bounds in structure data types. **CVE ID : CVE-2022-37453**	https://industrial.softing.com/fileadmin/psirt/downloads/syt-2022-9.html, https://softing.com	A-SOF-EDGE-051122/1992
Product: edgeconnector					
Affected Version(s): * Up to (including) 3.50					
Out-of-bounds Write	20-Oct-2022	7.5	An issue was discovered in Softing OPC UA C++ SDK before 6.10. A buffer overflow or an excess allocation happens due	https://industrial.softing.com/fileadmin/psirt/downloads/syt	A-SOF-EDGE-051122/1993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to unchecked array and matrix bounds in structure data types. **CVE ID : CVE-2022-37453**	-2022-9.html, https://softing.com	
Product: opc					
Affected Version(s): * Up to (including) 5.22					
Out-of-bounds Write	20-Oct-2022	7.5	An issue was discovered in Softing OPC UA C++ SDK before 6.10. A buffer overflow or an excess allocation happens due to unchecked array and matrix bounds in structure data types. **CVE ID : CVE-2022-37453**	https://industrial.softing.com/fileadmin/psirt/downloads/syt-2022-9.html, https://softing.com	A-SOF-OPC-051122/1994
Affected Version(s): From (including) 5.20 Up to (including) 5.22					
Use After Free	20-Oct-2022	7.5	An issue was discovered in Softing OPC UA C++ SDK 5.66 through 6.x before 6.10. An OPC/UA browse request exceeding the server limit on continuation points may cause a use-after-free error **CVE ID : CVE-2022-39823**	https://www.softing.com, https://industrial.softing.com/fileadmin/psirt/downloads/syt-2022-8.html	A-SOF-OPC-051122/1995
Product: opc_ua_c\+\+_software_development_kit					
Affected Version(s): * Up to (including) 6.00					
Out-of-bounds Write	20-Oct-2022	7.5	An issue was discovered in Softing OPC UA C++ SDK before 6.10. A buffer overflow or an excess allocation happens due to unchecked array and matrix bounds in structure data types.	https://industrial.softing.com/fileadmin/psirt/downloads/syt-2022-9.html, https://softing.com	A-SOF-OPC_-051122/1996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37453		
Affected Version(s): From (including) 5.70 Up to (including) 6.00					
Use After Free	20-Oct-2022	7.5	An issue was discovered in Softing OPC UA C++ SDK 5.66 through 6.x before 6.10. An OPC/UA browse request exceeding the server limit on continuation points may cause a use-after-free error **CVE ID : CVE-2022-39823**	https://www.softing.com, https://industrial.softing.com/fileadmin/psirt/downloads/syt-2022-8.html	A-SOF-OPC_-051122/1997
Product: secure_integration_server					
Affected Version(s): * Up to (including) 1.22					
Out-of-bounds Write	20-Oct-2022	7.5	An issue was discovered in Softing OPC UA C++ SDK before 6.10. A buffer overflow or an excess allocation happens due to unchecked array and matrix bounds in structure data types. **CVE ID : CVE-2022-37453**	https://industrial.softing.com/fileadmin/psirt/downloads/syt-2022-9.html, https://softing.com	A-SOF-SECU-051122/1998
Product: uagates					
Affected Version(s): * Up to (including) 1.74					
Out-of-bounds Write	20-Oct-2022	7.5	An issue was discovered in Softing OPC UA C++ SDK before 6.10. A buffer overflow or an excess allocation happens due to unchecked array and matrix bounds in structure data types. **CVE ID : CVE-2022-37453**	https://industrial.softing.com/fileadmin/psirt/downloads/syt-2022-9.html, https://softing.com	A-SOF-UAGA-051122/1999
Vendor: softmotions					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: iowow					
Affected Version(s): * Up to (including) 1.4.15					
Out-of-bounds Write	21-Oct-2022	7.5	IOWOW is a C utility library and persistent key/value storage engine. Versions 1.4.15 and prior contain a stack buffer overflow vulnerability that allows for Denial of Service (DOS) when it parses scientific notation numbers present in JSON. A patch for this issue is available at commit a79d31e4cff1d5a08f665574b29fd885897a28fd in the `master` branch of the repository. There are no workarounds other than applying the patch. **CVE ID : CVE-2022-23462**	https://securitylab.github.com/advisories/GHSL-2022-066_iowow/, https://github.com/Softmotions/iowow/commit/a79d31e4cff1d5a08f665574b29fd885897a28fd	A-SOF-IOWO-051122/2000
Vendor: softr					
Product: softr					
Affected Version(s): 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2022	6.1	Softr v2.0 was discovered to contain a Cross-Site Scripting (XSS) vulnerability via the First Name parameter under the Create A New Account module. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	N/A	A-SOF-SOFT-051122/2001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32407		
Vendor: Solarwinds					
Product: orion_platform					
Affected Version(s): * Up to (excluding) 2020.2.6					
Deserialization of Untrusted Data	20-Oct-2022	8.8	SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with valid access to SolarWinds Web Console to execute arbitrary commands. **CVE ID : CVE-2022-36958**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-36958	A-SOL-ORIO-051122/2002
Deserialization of Untrusted Data	20-Oct-2022	7.2	SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to SolarWinds Web Console to execute arbitrary commands. **CVE ID : CVE-2022-36957**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-36957	A-SOL-ORIO-051122/2003
Deserialization of Untrusted Data	20-Oct-2022	7.2	SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to SolarWinds Web Console to execute arbitrary commands.	https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-38108	A-SOL-ORIO-051122/2004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38108		
Authorization Bypass Through User-Controlled Key	20-Oct-2022	5.4	Users with Node Management rights were able to view and edit all nodes due to Insufficient control on URL parameter causing insecure direct object reference (IDOR) vulnerability in SolarWinds Platform 2022.3 and previous. **CVE ID : CVE-2022-36966**	https://documentation.solarwinds.com/en/success_center/orionplatform/content/release_notes/solarwinds_platform_2022-4_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-36966	A-SOL-ORIO-051122/2005
Affected Version(s): 2020.2.6					
Deserialization of Untrusted Data	20-Oct-2022	8.8	SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with valid access to SolarWinds Web Console to execute arbitrary commands. **CVE ID : CVE-2022-36958**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-36958	A-SOL-ORIO-051122/2006
Deserialization of Untrusted Data	20-Oct-2022	7.2	SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level	https://www.solarwinds.com/trust-center/security-advisories/C	A-SOL-ORIO-051122/2007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account access to SolarWinds Web Console to execute arbitrary commands. **CVE ID : CVE-2022-36957**	VE-2022-36957	
Deserialization of Untrusted Data	20-Oct-2022	7.2	SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to SolarWinds Web Console to execute arbitrary commands. **CVE ID : CVE-2022-38108**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-38108	A-SOL-ORIO-051122/2008
Authorization Bypass Through User-Controlled Key	20-Oct-2022	5.4	Users with Node Management rights were able to view and edit all nodes due to Insufficient control on URL parameter causing insecure direct object reference (IDOR) vulnerability in SolarWinds Platform 2022.3 and previous. **CVE ID : CVE-2022-36966**	https://documentation.solarwinds.com/en/success_center/orionplatform/content/release_notes/solarwinds_platform_2022-4_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-36966	A-SOL-ORIO-051122/2009
Affected Version(s): 2022.2					
Deserialization of	20-Oct-2022	8.8	SolarWinds Platform was susceptible to the	https://www.solarwind	A-SOL-ORIO-051122/2010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			Deserialization of Untrusted Data. This vulnerability allows a remote adversary with valid access to SolarWinds Web Console to execute arbitrary commands. **CVE ID : CVE-2022-36958**	s.com/trust-center/security-advisories/CVE-2022-36958	
Deserialization of Untrusted Data	20-Oct-2022	7.2	SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to SolarWinds Web Console to execute arbitrary commands. **CVE ID : CVE-2022-36957**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-36957	A-SOL-ORIO-051122/2011
Deserialization of Untrusted Data	20-Oct-2022	7.2	SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to SolarWinds Web Console to execute arbitrary commands. **CVE ID : CVE-2022-38108**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-38108	A-SOL-ORIO-051122/2012
Authorization Bypass Through User-	20-Oct-2022	5.4	Users with Node Management rights were able to view and edit all nodes due to Insufficient control on URL parameter causing	https://documentation.solarwinds.com/en/success_center/orionplatform/	A-SOL-ORIO-051122/2013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Key			insecure direct object reference (IDOR) vulnerability in SolarWinds Platform 2022.3 and previous. **CVE ID : CVE-2022-36966**	content/release_notes/solarwinds_platform_2022-4_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-36966	
Affected Version(s): 2022.3					
Deserialization of Untrusted Data	20-Oct-2022	8.8	SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with valid access to SolarWinds Web Console to execute arbitrary commands. **CVE ID : CVE-2022-36958**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-36958	A-SOL-ORIO-051122/2014
Deserialization of Untrusted Data	20-Oct-2022	7.2	SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to SolarWinds Web Console to execute arbitrary commands. **CVE ID : CVE-2022-36957**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-36957	A-SOL-ORIO-051122/2015
Deserialization of	20-Oct-2022	7.2	SolarWinds Platform was susceptible to the	https://www.solarwind	A-SOL-ORIO-051122/2016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to SolarWinds Web Console to execute arbitrary commands. **CVE ID : CVE-2022-38108**	s.com/trust-center/security-advisories/CVE-2022-38108	
Authorization Bypass Through User-Controlled Key	20-Oct-2022	5.4	Users with Node Management rights were able to view and edit all nodes due to Insufficient control on URL parameter causing insecure direct object reference (IDOR) vulnerability in SolarWinds Platform 2022.3 and previous. **CVE ID : CVE-2022-36966**	https://documentation.solarwinds.com/en/success_center/orionplatform/content/release_notes/solarwinds_platform_2022-4_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-36966	A-SOL-ORIO-051122/2017
Product: sql_sentry					
Affected Version(s): * Up to (including) 2021.18.10					
Generation of Error Message Containing Sensitive Information	19-Oct-2022	5.3	Sensitive information could be displayed when a detailed technical error message is posted. This information could disclose environmental details. **CVE ID : CVE-2022-38107**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-38107, https://docs	A-SOL-SQL_-051122/2018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				.sentryone.com/help/sentryone-platform-release-notes	
Vendor: Sony					
Product: content_transfer					
Affected Version(s): * Up to (including) 1.3					
Untrusted Search Path	24-Oct-2022	7.8	Untrusted search path vulnerability in the installer of Content Transfer (for Windows) Ver.1.3 and prior allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2022-41796**	https://www.sony.jp/support/audiosoftware/contenttransfer/	A-SON-CONT-051122/2019
Vendor: sra-admin_project					
Product: sra-admin					
Affected Version(s): * Up to (including) 1.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2022	5.4	sra-admin is a background rights management system that separates the front and back end. sra-admin version 1.1.1 has a storage cross-site scripting (XSS) vulnerability. After logging into the sra-admin background, an attacker can upload an html page containing xss attack code in "Personal Center" - "Profile Picture Upload" allowing theft of the user's personal information. This issue	https://github.com/momofoolish/sra-admin/security/advisories/GHSA-v7r9-qx74-h3v8	A-SRA-SRA--051122/2020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been patched in 1.1.2. There are no known workarounds. **CVE ID : CVE-2022-39301**		
Vendor: ST					
Product: stm32_mw_usb_host					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-Oct-2022	9.8	A buffer overflow vulnerability in stm32_mw_usb_host of STMicroelectronics allows an attacker to execute arbitrary code when the descriptor contains more endpoints than USBH_MAX_NUM_ENDPOINTS. The library is typically integrated when using a RTOS such as FreeRTOS on STM32 MCUs. **CVE ID : CVE-2021-42553**	https://github.com/STMicroelectronics/stm32_mw_usb_host/pull/4	A-ST-STM3-051122/2021
Vendor: superwhite					
Product: demon_image_annotation					
Affected Version(s): * Up to (excluding) 4.8					
Cross-Site Request Forgery (CSRF)	28-Oct-2022	8.8	The demon image annotation plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.7. This is due to missing nonce validation in the ~/includes/settings.php file. This makes it possible for unauthenticated attackers to modify the	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2772352%40demon-image-annotation&new=2772352%40demo	A-SUP-DEMO-051122/2022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plugin's settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2022-2864**	n-image-annotation&sfp_email=&sfph_mail=	
Vendor: synacor					
Product: zimbra_collaboration_suite					
Affected Version(s): * Up to (including) 9.0.0					
Improper Privilege Management	17-Oct-2022	7.8	Due to an issue with incorrect sudo permissions, Zimbra Collaboration Suite (ZCS) suffers from a local privilege escalation issue in versions 9.0.0 and prior, where the 'zimbra' user can effectively coerce postfix into running arbitrary commands as 'root'. **CVE ID : CVE-2022-3569**	https://github.com/rapid7/metasploit-framework/pull/17141	A-SYN-ZIMB-051122/2023
Vendor: Synology					
Product: diskstation_manager					
Affected Version(s): * Up to (excluding) 7.1-42661					
Missing Authentication for Critical Function	25-Oct-2022	9.1	Missing authentication for critical function vulnerability in iSCSI management functionality in Synology DiskStation Manager (DSM) before 7.1-42661 allows remote attackers to read or write arbitrary	https://www.synology.com/security/advisory/Synology_SA_22_18	A-SYN-DISK-051122/2024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files via unspecified vectors. **CVE ID : CVE-2022-27623**		
Server-Side Request Forgery (SSRF)	25-Oct-2022	4.3	Server-Side Request Forgery (SSRF) vulnerability in Package Center functionality in Synology DiskStation Manager (DSM) before 7.1-42661 allows remote authenticated users to access intranet resources via unspecified vectors. **CVE ID : CVE-2022-27622**	https://www.synology.com/security/advisory/Synology_SA_22_18	A-SYN-DISK-051122/2025
Affected Version(s): * Up to (excluding) 7.1.1-42962-2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-2022	9.8	A vulnerability regarding improper restriction of operations within the bounds of a memory buffer is found in the packet decryption functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-27624**	https://www.synology.com/security/advisory/Synology_SA_22_17	A-SYN-DISK-051122/2026
Improper Restriction of	20-Oct-2022	9.8	A vulnerability regarding improper restriction of operations within the	https://www.synology.com/security	A-SYN-DISK-051122/2027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			bounds of a memory buffer is found in the message processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-27625**	/advisory/Synology_SA_22_17	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	20-Oct-2022	8.1	A vulnerability regarding concurrent execution using shared resource with improper synchronization ('Race Condition') is found in the session processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-27626**	https://www.synology.com/security/advisory/Synology_SA_22_17	A-SYN-DISK-051122/2028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-2022	7.5	A vulnerability regarding out-of-bounds read is found in the session processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to obtain sensitive information via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-3576**	https://www.synology.com/security/advisory/Synology_SA_22_17	A-SYN-DISK-051122/2029
Product: presto_file_server					
Affected Version(s): * Up to (excluding) 2.1.2-1601					
Improper Privilege Management	26-Oct-2022	8.8	Improper privilege management vulnerability in summary report management in Synology Presto File Server before 2.1.2-1601 allows remote authenticated users to bypass security constraint via unspecified vectors. **CVE ID : CVE-2022-43749**	https://www.synology.com/security/advisory/Synology_SA_22_19	A-SYN-PRES-051122/2030
Improper Limitation of a Pathname to a Restricted Directory ('Path	26-Oct-2022	7.5	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in file operation management in Synology Presto File Server before 2.1.2-1601 allows	https://www.synology.com/security/advisory/Synology_SA_22_19	A-SYN-PRES-051122/2031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Traversal')			remote attackers to write arbitrary files via unspecified vectors. **CVE ID : CVE-2022-43748**		
Vendor: tableau					
Product: tableau_server					
Affected Version(s): From (including) 2020.4 Up to (including) 2020.4.20					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Oct-2022	9.8	Tableau discovered a path traversal vulnerability affecting Tableau Server Administration Agent's internal file transfer service that could allow remote code execution.Tableau only supports product versions for 24 months after release. Older versions have reached their End of Life and are no longer supported. They are also not assessed for potential security issues and do not receive security updates. **CVE ID : CVE-2022-22128**	https://kb.tableau.com/articles/Issue/issue-affecting-tableau-server-administration-agent	A-TAB-TABL-051122/2032
Affected Version(s): From (including) 2021.1 Up to (including) 2021.1.17					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Oct-2022	9.8	Tableau discovered a path traversal vulnerability affecting Tableau Server Administration Agent's internal file transfer service that could allow remote code execution.Tableau only supports product	https://kb.tableau.com/articles/Issue/issue-affecting-tableau-server-administration-agent	A-TAB-TABL-051122/2033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions for 24 months after release. Older versions have reached their End of Life and are no longer supported. They are also not assessed for potential security issues and do not receive security updates. **CVE ID : CVE-2022-22128**		
Affected Version(s): From (including) 2021.2 Up to (including) 2021.2.15					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Oct-2022	9.8	Tableau discovered a path traversal vulnerability affecting Tableau Server Administration Agent's internal file transfer service that could allow remote code execution.Tableau only supports product versions for 24 months after release. Older versions have reached their End of Life and are no longer supported. They are also not assessed for potential security issues and do not receive security updates. **CVE ID : CVE-2022-22128**	https://kb.tableau.com/articles/Issue/issue-affecting-tableau-server-administration-agent	A-TAB-TABL-051122/2034
Affected Version(s): From (including) 2021.3 Up to (including) 2021.3.14					
Improper Limitation of a Pathname to a Restricted	17-Oct-2022	9.8	Tableau discovered a path traversal vulnerability affecting Tableau Server Administration Agent's internal file transfer	https://kb.tableau.com/articles/Issue/issue-affecting-tableau-	A-TAB-TABL-051122/2035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			service that could allow remote code execution.Tableau only supports product versions for 24 months after release. Older versions have reached their End of Life and are no longer supported. They are also not assessed for potential security issues and do not receive security updates. **CVE ID : CVE-2022-22128**	server-administration-agent	
Affected Version(s): From (including) 2021.4 Up to (including) 2021.4.9					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Oct-2022	9.8	Tableau discovered a path traversal vulnerability affecting Tableau Server Administration Agent's internal file transfer service that could allow remote code execution.Tableau only supports product versions for 24 months after release. Older versions have reached their End of Life and are no longer supported. They are also not assessed for potential security issues and do not receive security updates. **CVE ID : CVE-2022-22128**	https://kb.tableau.com/articles/Issue/issue-affecting-tableau-server-administration-agent	A-TAB-TABL-051122/2036
Affected Version(s): From (including) 2022.1 Up to (including) 2022.1.4					
Improper Limitatio	17-Oct-2022	9.8	Tableau discovered a path traversal	https://kb.tableau.com/a	A-TAB-TABL-051122/2037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n of a Pathname to a Restricted Directory ('Path Traversal')			vulnerability affecting Tableau Server Administration Agent's internal file transfer service that could allow remote code execution.Tableau only supports product versions for 24 months after release. Older versions have reached their End of Life and are no longer supported. They are also not assessed for potential security issues and do not receive security updates. **CVE ID : CVE-2022-22128**	rticles/Issue/issue-affecting-tableau-server-administration-agent	
Vendor: tasks					
Product: tasks					
Affected Version(s): * Up to (excluding) 12.7.1					
Exposure of Resource to Wrong Sphere	25-Oct-2022	5.5	The Tasks.org Android app is an open-source app for to-do lists and reminders. The Tasks.org app uses the activity `ShareLinkActivity.kt` to handle "share" intents coming from other components in the same device and convert them to tasks. Those intents may contain arbitrary file paths as attachments, in which case the files pointed by those paths are copied in the app's external storage directory. Prior to versions 12.7.1 and	https://github.com/tasks/tasks/security/advisories/GHSA-8x58-cg74-8jg8, https://github.com/tasks/tasks/commit/23bf69d3f44b07e4bc62ea107f72103239f5d942	A-TAS-TASK-051122/2038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13.0.1, those paths were not validated, allowing a malicious or compromised application in the same device to force Tasks.org to copy files from its internal storage to its external storage directory, where they became accessible to any component with permission to read the external storage. This vulnerability can lead to sensitive information disclosure. All information in the user's notes and the app's preferences, including the encrypted credentials of CalDav integrations if enabled, could be accessed by third party applications installed on the same device. This issue was fixed in versions 12.7.1 and 13.0.1. There are no known workarounds. **CVE ID : CVE-2022-39349**		
Affected Version(s): 13.0.0					
Exposure of Resource to Wrong Sphere	25-Oct-2022	5.5	The Tasks.org Android app is an open-source app for to-do lists and reminders. The Tasks.org app uses the activity `ShareLinkActivity.kt` to handle "share" intents coming from other components in the same device and convert them to tasks. Those intents	https://github.com/tasks/tasks/security/advisories/GHSA-8x58-cg74-8jg8, https://github.com/tasks/tasks/commit/23bf69d	A-TAS-TASK-051122/2039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may contain arbitrary file paths as attachments, in which case the files pointed by those paths are copied in the app's external storage directory. Prior to versions 12.7.1 and 13.0.1, those paths were not validated, allowing a malicious or compromised application in the same device to force Tasks.org to copy files from its internal storage to its external storage directory, where they became accessible to any component with permission to read the external storage. This vulnerability can lead to sensitive information disclosure. All information in the user's notes and the app's preferences, including the encrypted credentials of CalDav integrations if enabled, could be accessed by third party applications installed on the same device. This issue was fixed in versions 12.7.1 and 13.0.1. There are no known workarounds. **CVE ID : CVE-2022-39349**	3f44b07e4bc62ea107f72103239f5d942	
Vendor: Tech-banker					
Product: contact_bank					
Affected Version(s): * Up to (including) 3.0.30					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2022	4.8	The Contact Bank WordPress plugin through 3.0.30 does not sanitise and escape some of its Form settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-3350**	N/A	A-TEC-CONT-051122/2040
Vendor: Tenable					
Product: nessus					
Affected Version(s): *					
Insufficiently Protected Credentials	17-Oct-2022	6.5	Insufficiently Protected Credentials: An authenticated user with debug privileges can retrieve stored Nessus policy credentials from the “nessusd” process in cleartext via process dumping. The affected products are all versions of Nessus Essentials and Professional. The vulnerability allows an attacker to access credentials stored in Nessus scanners, potentially compromising its customers’ network of assets. **CVE ID : CVE-2022-28291**	N/A	A-TEN-NESS-051122/2041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 10.2.0					
Improper Privilege Management	25-Oct-2022	6.5	An authenticated attacker could read Nessus Debug Log file attachments from the web UI without having the correct privileges to do so. This may lead to the disclosure of information on the scan target and/or the Nessus scan to unauthorized parties able to reach the Nessus instance. **CVE ID : CVE-2022-33757**	https://www.tenable.com/security/tns-2022-11	A-TEN-NESS-051122/2042
Vendor: themepoints					
Product: testimonials					
Affected Version(s): * Up to (including) 2.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-2022	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Themepoints Testimonials plugin <= 2.6 on WordPress. **CVE ID : CVE-2021-36858**	https://patchstack.com/database/vulnerability/super-testimonial/wordpress-testimonials-plugin-2-6-auth-stored-cross-site-scripting-xss-vulnerability?_s_id=cve, https://wordpress.org/plugins/super-testimonial/	A-THE-TEST-051122/2043
Vendor: themeum					
Product: tutor_lms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.0.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2022	4.8	The Tutor LMS WordPress plugin before 2.0.10 does not escape some course parameters, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2563**	N/A	A-THE-TUTO-051122/2044
Vendor: train_scheduler_app_project					
Product: train_scheduler_app					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2022	5.4	Multiple stored cross-site scripting (XSS) vulnerabilities in Train Scheduler App v1.0 allow attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Train Code, Train Name, and Destination text fields. **CVE ID : CVE-2022-42992**	N/A	A-TRA-TRAI-051122/2045
Vendor: trumpf					
Product: job_order_interface					
Affected Version(s): *					
N/A	17-Oct-2022	9.8	Multiple Trumpf Products in multiple versions use default privileged Windows users and passwords. An	https://cert.vde.com/en/advisories/VDE-2022-023/	A-TRU-JOB_-051122/2046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adversary may use these accounts to remotely gain full access to the system. **CVE ID : CVE-2022-2052**		
Product: oseon					
Affected Version(s): * Up to (including) 1.6					
N/A	17-Oct-2022	9.8	Multiple Trumpf Products in multiple versions use default privileged Windows users and passwords. An adversary may use these accounts to remotely gain full access to the system. **CVE ID : CVE-2022-2052**	https://cert.vde.com/en/advisories/VDE-2022-023/	A-TRU-OSEO-051122/2047
Product: trutops_boost					
Affected Version(s): *					
N/A	17-Oct-2022	9.8	Multiple Trumpf Products in multiple versions use default privileged Windows users and passwords. An adversary may use these accounts to remotely gain full access to the system. **CVE ID : CVE-2022-2052**	https://cert.vde.com/en/advisories/VDE-2022-023/	A-TRU-TRUT-051122/2048
Product: trutops_fab					
Affected Version(s): *					
N/A	17-Oct-2022	9.8	Multiple Trumpf Products in multiple versions use default privileged Windows users and passwords. An adversary may use these	https://cert.vde.com/en/advisories/VDE-2022-023/	A-TRU-TRUT-051122/2049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accounts to remotely gain full access to the system. **CVE ID : CVE-2022-2052**		
Product: trutops_monitor					
Affected Version(s): *					
N/A	17-Oct-2022	9.8	Multiple Trumpf Products in multiple versions use default privileged Windows users and passwords. An adversary may use these accounts to remotely gain full access to the system. **CVE ID : CVE-2022-2052**	https://cert.vde.com/en/advisories/VDE-2022-023/	A-TRU-TRUT-051122/2050
Vendor: twistedmatrix					
Product: twisted					
Affected Version(s): 22.10.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2022	5.4	Twisted is an event-based framework for internet applications. Started with version 0.9.4, when the host header does not match a configured host `twisted.web.vhost.NameVirtualHost` will return a `NoResource` resource which renders the Host header unescaped into the 404 response allowing HTML and script injection. In practice this should be very difficult to exploit as being able to modify the Host header of a normal HTTP request implies	https://github.com/twisted/twisted/commit/f2f5e81c03f14e253e85fe457e646130780db40b, https://github.com/twisted/twisted/security/advisories/GHSA-vg46-2rrj-3647, https://github.com/twisted/twisted/commit/f49041bb67792	A-TWI-TWIS-051122/2051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that one is already in a privileged position. This issue was fixed in version 22.10.0rc1. There are no known workarounds. **CVE ID : CVE-2022-39348**	506d85aeda9cf6157e92f8048f4	
Affected Version(s): From (including) 0.9.4 Up to (excluding) 22.10.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2022	5.4	Twisted is an event-based framework for internet applications. Started with version 0.9.4, when the host header does not match a configured host `twisted.web.vhost.NameVirtualHost` will return a `NoResource` resource which renders the Host header unescaped into the 404 response allowing HTML and script injection. In practice this should be very difficult to exploit as being able to modify the Host header of a normal HTTP request implies that one is already in a privileged position. This issue was fixed in version 22.10.0rc1. There are no known workarounds. **CVE ID : CVE-2022-39348**	https://github.com/twisted/twisted/commit/f2f5e81c03f14e253e85fe457e646130780db40b, https://github.com/twisted/twisted/security/advisories/GHSA-vg46-2rrj-3647, https://github.com/twisted/twisted/commit/f49041bb67792506d85aeda9cf6157e92f8048f4	A-TWI-TWIS-051122/2052
Vendor: uatech					
Product: badaso					
Affected Version(s): 2.6.0					
Unrestricted Upload of File	25-Oct-2022	9.8	Badaso version 2.6.0 allows an unauthenticated remote	N/A	A-UAT-BADA-051122/2053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Dangerous Type			attacker to execute arbitrary code remotely on the server. This is possible because the application does not properly validate the data uploaded by users. **CVE ID : CVE-2022-41711**		
Vendor: uglifyjs_project					
Product: uglifyjs					
Affected Version(s): 3.13.2					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	20-Oct-2022	9.8	Prototype pollution vulnerability in function DEFNODE in ast.js in mishoo UglifyJS 3.13.2 via the name variable in ast.js. **CVE ID : CVE-2022-37598**	N/A	A-UGL-UGLI-051122/2054
Vendor: Vestacp					
Product: control_panel					
Affected Version(s): * Up to (excluding) 0.9.8-26-43					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Oct-2022	7.2	myVesta Control Panel before 0.9.8-26-43 and Vesta Control Panel before 0.9.8-26 are vulnerable to command injection. An authenticated and remote administrative user can execute arbitrary commands via the v_sftp_license parameter when sending HTTP POST requests to	https://github.com/myvesta/vesta/commit/7991753ab7c5c568768028fb77554db8ea149f17, https://github.com/serghey-rodin/vesta/commit/a4e	A-VES-CONT-051122/2055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the /edit/server endpoint. **CVE ID : CVE-2021-46850**	4542a6d1351c2857b169f8621dd9a13a2e896	
Product: vesta_control_panel					
Affected Version(s): * Up to (excluding) 0.9.8-26					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Oct-2022	7.2	myVesta Control Panel before 0.9.8-26-43 and Vesta Control Panel before 0.9.8-26 are vulnerable to command injection. An authenticated and remote administrative user can execute arbitrary commands via the v_sftp_license parameter when sending HTTP POST requests to the /edit/server endpoint. **CVE ID : CVE-2021-46850**	https://github.com/myvesta/vesta/commit/7991753ab7c5c568768028fb77554db8ea149f17, https://github.com/serghey-rodin/vesta/commit/a4e4542a6d1351c2857b169f8621dd9a13a2e896	A-VES-VEST-051122/2056
Vendor: VIM					
Product: vim					
Affected Version(s): * Up to (excluding) 9.0.0805					
Use After Free	26-Oct-2022	7.5	A vulnerability was found in vim and classified as problematic. Affected by this issue is the function qf_update_buffer of the file quickfix.c of the component autocmd Handler. The manipulation leads to use after free. The attack may be launched remotely. Upgrading to version 9.0.0805 is able to address this issue. The	https://github.com/vim/vim/commit/d0fab10ed2a86698937e3c3fed2f10bd9bb5e731	A-VIM-VIM-051122/2057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			name of the patch is d0fab10ed2a86698937e3c3fed2f10bd9bb5e731. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-212324. **CVE ID : CVE-2022-3705**		
Vendor: Vmware					
Product: cloud_foundation					
Affected Version(s): * Up to (excluding) 3.11					
Improper Restriction of XML External Entity Reference	28-Oct-2022	9.1	VMware Cloud Foundation (NSX-V) contains an XML External Entity (XXE) vulnerability. On VCF 3.x instances with NSX-V deployed, this may allow a user to exploit this issue leading to a denial-of-service condition or unintended information disclosure. **CVE ID : CVE-2022-31678**	https://www.vmware.com/security/advisories/VMSA-2022-0027.html	A-VMW-CLOU-051122/2058
Product: nsx_data_center					
Affected Version(s): * Up to (excluding) 6.4.14					
Improper Restriction of XML External Entity Reference	28-Oct-2022	9.1	VMware Cloud Foundation (NSX-V) contains an XML External Entity (XXE) vulnerability. On VCF 3.x instances with NSX-V deployed, this may allow a user to exploit this issue leading to a denial-of-service condition or	https://www.vmware.com/security/advisories/VMSA-2022-0027.html	A-VMW-NSX_-051122/2059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unintended information disclosure. **CVE ID : CVE-2022-31678**		
Vendor: web-based_student_clearance_system_project					
Product: web-based_student_clearance_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2022	8.8	A vulnerability was found in SourceCodester Web-Based Student Clearance System. It has been classified as critical. This affects an unknown part of the file Admin/edit-admin.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212415. **CVE ID : CVE-2022-3733**	N/A	A-WEB-WEB--051122/2060
Vendor: Webmin					
Product: usermin					
Affected Version(s): * Up to (including) 1.850					
Improper Neutralization of Special Elements used in an OS Command ('OS	25-Oct-2022	8.8	Usermin through 1.850 allows a remote authenticated user to execute OS commands via command injection in a filename for the GPG module. **CVE ID : CVE-2022-35132**	https://webmin.com/uchanges.html	A-WEB-USER-051122/2061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')					
Vendor: weseek					
Product: growi					
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.5.25					
Missing Authorization	24-Oct-2022	6.5	Improper access control vulnerability in GROWI prior to v5.1.4 (v5 series) and versions prior to v4.5.25 (v4 series) allows a remote authenticated attacker to bypass access restriction and download the markdown data from the pages set to private by the other users. **CVE ID : CVE-2022-41799**	https://weseek.co.jp/en/news/2022/10/07/growi-private-page-can-be-viewed/	A-WES-GROW-051122/2062
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.1.4					
Missing Authorization	24-Oct-2022	6.5	Improper access control vulnerability in GROWI prior to v5.1.4 (v5 series) and versions prior to v4.5.25 (v4 series) allows a remote authenticated attacker to bypass access restriction and download the markdown data from the pages set to private by the other users. **CVE ID : CVE-2022-41799**	https://weseek.co.jp/en/news/2022/10/07/growi-private-page-can-be-viewed/	A-WES-GROW-051122/2063
Vendor: wintercms					
Product: winter					
Affected Version(s): 1.1.8					
Improperly Controlled Modificati	26-Oct-2022	9.8	Winter is a free, open-source content management system based on the Laravel PHP framework. The	https://github.com/wintercms/winter/commit/2a13faf99972	A-WIN-WINT-051122/2064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on of Object Prototype Attributes ('Prototype Pollution')			Snowboard framework in versions 1.1.8, 1.1.9, and 1.2.0 is vulnerable to prototype pollution in the main Snowboard class as well as its plugin loader. The 1.0 branch of Winter is not affected, as it does not contain the Snowboard framework. This issue has been patched in v1.1.10 and v1.2.1. As a workaround, one may avoid this issue by following some common security practices for JavaScript, including implementing a content security policy and auditing scripts. **CVE ID : CVE-2022-39357**	e84c9661258f16c4750fa99d29a1, https://github.com/wintercms/winter/commit/bce4b59584abf961e9400af3d7a4fd7638e26c7f, https://github.com/wintercms/winter/security/advisories/GHSA-3fh5-q6fg-w28q	
Affected Version(s): 1.1.9					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	26-Oct-2022	9.8	Winter is a free, open-source content management system based on the Laravel PHP framework. The Snowboard framework in versions 1.1.8, 1.1.9, and 1.2.0 is vulnerable to prototype pollution in the main Snowboard class as well as its plugin loader. The 1.0 branch of Winter is not affected, as it does not contain the Snowboard framework. This issue has been patched in v1.1.10 and v1.2.1. As a workaround, one may avoid this issue by following some	https://github.com/wintercms/winter/commit/2a13faf99972e84c9661258f16c4750fa99d29a1, https://github.com/wintercms/winter/commit/bce4b59584abf961e9400af3d7a4fd7638e26c7f, https://github.com/wintercms/winter/security/a	A-WIN-WINT-051122/2065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			common security practices for JavaScript, including implementing a content security policy and auditing scripts. **CVE ID : CVE-2022-39357**	dvisories/GHSA-3fh5-q6fg-w28q	
Affected Version(s): 1.2.0					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	26-Oct-2022	9.8	Winter is a free, open-source content management system based on the Laravel PHP framework. The Snowboard framework in versions 1.1.8, 1.1.9, and 1.2.0 is vulnerable to prototype pollution in the main Snowboard class as well as its plugin loader. The 1.0 branch of Winter is not affected, as it does not contain the Snowboard framework. This issue has been patched in v1.1.10 and v1.2.1. As a workaround, one may avoid this issue by following some common security practices for JavaScript, including implementing a content security policy and auditing scripts. **CVE ID : CVE-2022-39357**	https://github.com/wintercms/winter/commit/2a13faf99972e84c9661258f16c4750fa99d29a1, https://github.com/wintercms/winter/commit/bce4b59584abf961e9400af3d7a4fd7638e26c7f, https://github.com/wintercms/winter/security/advisories/GHSA-3fh5-q6fg-w28q	A-WIN-WINT-051122/2066
Vendor: wire					
Product: wire_server					
Affected Version(s): * Up to (excluding) 2022-07-12					
Improper Authentication	18-Oct-2022	8.1	Wire is an encrypted communication and collaboration platform.	https://github.com/wireapp/wire-	A-WIR-WIRE-051122/2067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Versions prior to 2022-07-12/Chart 4.19.0 are subject to Token Recipient Confusion. If an attacker has certain details of SAML IdP metadata, and configures their own SAML on the same backend, the attacker can delete all SAML authenticated accounts of a targeted team, Authenticate as a user of the attacked team and create arbitrary accounts in the context of the team if it is not managed by SCIM. This issue is fixed in wire-server 2022-07-12 and is already deployed on all Wire managed services. On-premise instances of wire-server need to be updated to 2022-07-12/Chart 4.19.0, so that their backends are no longer affected. As a workaround, the risk of an attack can be reduced by disabling SAML configuration for teams (galley.config.settings.featureFlags.sso). Helm overrides are located in `values/wire-server/values.yaml` Note that the ability to configure SAML SSO as a team is disabled by default for on-premise installations.	server/security/advisories/GHSA-gq27-gmgq-fmxw	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31122		
Vendor: wisa					
Product: smart_wing_cms					
Affected Version(s): * Up to (excluding) 19051					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Oct-2022	9.8	This vulnerability could allow a remote attacker to execute remote commands with improper validation of parameters of certain API constructors. Remote attackers could use this vulnerability to execute malicious commands such as directory traversal. **CVE ID : CVE-2022-23770**	N/A	A-WIS-SMAR-051122/2068
Vendor: withsecure					
Product: f-secure_policy_manager					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2022	6.1	Reflected cross-site scripting (XSS) vulnerabilities in WithSecure through 2022-08-10) exists within the F-Secure Policy Manager due to an unvalidated parameter in the endpoint, which allows remote attackers to provide a malicious input. **CVE ID : CVE-2022-38162**	https://withsecure.com	A-WIT-F-SE-051122/2069
Vendor: wp_custom_cursors_project					
Product: wp_custom_cursors					
Affected Version(s): * Up to (excluding) 3.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	17-Oct-2022	6.1	The WP Custom Cursors WordPress plugin before 3.0.1 does not have CSRF check in place when creating and editing cursors, which could allow attackers to made a logged in admin perform such actions via CSRF attacks. Furthermore, due to the lack of sanitisation and escaping in some of the cursor options, it could also lead to Stored Cross-Site Scripting **CVE ID : CVE-2022-3149**	https://wpscan.com/vulnerability/4c13a93d-2100-4721-8937-a1205378655f	A-WP_-WP_C-051122/2070
Cross-Site Request Forgery (CSRF)	17-Oct-2022	4.3	The WP Custom Cursors WordPress plugin before 3.0.1 does not have CSRF check in place when deleting cursors, which could allow attackers to made a logged in admin delete arbitrary cursors via a CSRF attack. **CVE ID : CVE-2022-3151**	https://wpscan.com/vulnerability/27816c70-58ad-4ffb-adcc-69eb1b210744	A-WP_-WP_C-051122/2071
Affected Version(s): * Up to (including) 3.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Oct-2022	7.2	The WP Custom Cursors WordPress plugin through 3.0 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privileged users such as admin **CVE ID : CVE-2022-3150**	N/A	A-WP_-WP_C-051122/2072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wp_humans.txt_project					
Product: wp_humans.txt					
Affected Version(s): * Up to (including) 1.06					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2022	4.8	The WP Humans.txt WordPress plugin through 1.0.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-3392**	https://wpscan.com/vulnerability/2296156e-b177-478e-a01c-b1ea4fee0aca	A-WP_-WP_H-051122/2073
Vendor: X.org					
Product: libx11					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	17-Oct-2022	7.5	A vulnerability has been found in X.org libX11 and classified as problematic. This vulnerability affects the function _XimRegisterIMInstantiateCallback of the file modules/im/ximcp/imsClbk.c. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. VDB-211054 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3554**	https://cgit.freedesktop.org/xorg/lib/libX11/commit/?id=1d11822601fd24a396b354fa616b04ed3df8b4ef	A-X.O-LIBX-051122/2074
Affected Version(s): * Up to (excluding) 1.7.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	17-Oct-2022	7.5	A vulnerability was found in X.org libX11 and classified as problematic. This issue affects the function _XFreeX11XCBStructure of the file xcb_disp.c. The manipulation of the argument dpy leads to memory leak. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211055. **CVE ID : CVE-2022-3555**	https://cgit.freedesktop.org/xorg/lib/libX11/commit/?id=8a368d808fec166b5fb3dfe6312aab22c7ee20af	A-X.O-LIBX-051122/2075
Product: x_server					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Oct-2022	9.8	A vulnerability classified as critical was found in X.org Server. Affected by this vulnerability is the function _GetCountedString of the file xkb/xkb.c. The manipulation leads to buffer overflow. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211051. **CVE ID : CVE-2022-3550**	https://cgit.freedesktop.org/xorg/xserver/commit/?id=11beef0b7f1ed290348e45618e5fa0d2bffcb72e	A-X.O-X_SE-051122/2076
Missing Release of Memory after Effective Lifetime	17-Oct-2022	7.5	A vulnerability, which was classified as problematic, has been found in X.org Server. Affected by this issue is the function ProcXkbGetKbdByName	https://cgit.freedesktop.org/xorg/xserver/commit/?id=18f91b950e22c2a342a4fbc55e9	A-X.O-X_SE-051122/2077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the file xkb/xkb.c. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211052. **CVE ID : CVE-2022-3551**	ddf7534a707d2	
Improper Resource Shutdown or Release	17-Oct-2022	7.5	A vulnerability, which was classified as problematic, was found in X.org Server. This affects an unknown part of the file hw/xquartz/X11Controller.m of the component xquartz. The manipulation leads to denial of service. It is recommended to apply a patch to fix this issue. The identifier VDB-211053 was assigned to this vulnerability. **CVE ID : CVE-2022-3553**	https://cgit.freedesktop.org/xorg/xserver/commit/?id=dfd057996b26420309c324ec844a5ba6dd07eda3	A-X.O-X_SE-051122/2078
Vendor: xbifrost					
Product: bifrost					
Affected Version(s): * Up to (including) 1.8.6					
Improper Authentication	19-Oct-2022	8.8	Bifrost is a heterogeneous middleware that synchronizes MySQL, MariaDB to Redis, MongoDB, ClickHouse, MySQL and other services for production environments. Versions prior to 1.8.8-release are subject to authentication	https://github.com/brokercap/Bifrost/security/advisories/GHSA-mxrx-fg8p-5p5j	A-XBI-BIFR-051122/2079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass in the admin and monitor user groups by deleting the X-Requested-With: XMLHttpRequest field in the request header. This issue has been patched in 1.8.8-release. There are no known workarounds. **CVE ID : CVE-2022-39267**		
Vendor: Yokogawa					
Product: wtviewerefree					
Affected Version(s): From (including) 1.01 Up to (excluding) 1.53					
Out-of-bounds Write	24-Oct-2022	9.8	Stack-based buffer overflow in WTViewerE series WTViewerE 761941 from 1.31 to 1.61 and WTViewerEfree from 1.01 to 1.52 allows an attacker to cause the product to crash by processing a long file name. **CVE ID : CVE-2022-40984**	https://cdn.aff.yokogawa.com/8/756/details/Vulnerability_in_YOKOGAWA_application_software_WTViewerE_r0_e.pdf	A-YOK-WTVI-051122/2080
Product: wtviewere_761941					
Affected Version(s): From (including) 1.31 Up to (excluding) 1.62					
Out-of-bounds Write	24-Oct-2022	9.8	Stack-based buffer overflow in WTViewerE series WTViewerE 761941 from 1.31 to 1.61 and WTViewerEfree from 1.01 to 1.52 allows an attacker to cause the product to crash by processing a long file name. **CVE ID : CVE-2022-40984**	https://cdn.aff.yokogawa.com/8/756/details/Vulnerability_in_YOKOGAWA_application_software_WTViewerE_r0_e.pdf	A-YOK-WTVI-051122/2081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: yordam					
Product: library_automation_system					
Affected Version(s): * Up to (excluding) 19.02					
Exposure of Sensitive Information to an Unauthorized Actor	27-Oct-2022	7.5	Yordam Library Information Document Automation product before version 19.02 has an unauthenticated Information disclosure vulnerability. **CVE ID : CVE-2021-45475**	https://www.usom.gov.tr/bildirim/tr-22-0669	A-YOR-LIBR-051122/2082
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2022	6.1	Yordam Library Information Document Automation product before version 19.02 has an unauthenticated reflected XSS vulnerability. **CVE ID : CVE-2021-45476**	https://www.usom.gov.tr/bildirim/tr-22-0669	A-YOR-LIBR-051122/2083
Vendor: zalando					
Product: skipper					
Affected Version(s): * Up to (excluding) 0.13.237					
Server-Side Request Forgery (SSRF)	25-Oct-2022	9.8	Zalando Skipper v0.13.236 is vulnerable to Server-Side Request Forgery (SSRF). **CVE ID : CVE-2022-38580**	http://zalando.com	A-ZAL-SKIP-051122/2084
Hardware					
Vendor: Acer					
Product: altos_w2000h-w570h_f4					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2022	9.8	Acer Altos W2000h-W570h F4 R01.03.0018 was discovered to contain a stack overflow in the RevserveMem component. This vulnerability allows attackers to cause a Denial of Service (DoS) via injecting crafted shellcode into the NVRAM variable. **CVE ID : CVE-2022-41415**	http://acer.com	H-ACE-ALTO-071122/2085
Vendor: Asus					
Product: rt-n12e					
Affected Version(s): -					
Missing Authentication for Critical Function	19-Oct-2022	7.5	Asus RT-N12E 2.0.0.39 is affected by an incorrect access control vulnerability. Through system.asp / start_apply.htm, an attacker can change the administrator password without any authentication. **CVE ID : CVE-2020-23648**	https://www.asus.com/Networking/RTN12E/HelpDesk_BIOS/	H-ASU-RT-N-071122/2086
Vendor: bosch					
Product: videojet_multi_4000					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site	27-Oct-2022	4.8	Incomplete filtering of JavaScript code in different configuration fields of the web based interface of the VIDEOJET multi 4000 allows an attacker with administrative credentials to store	https://psirt.bosch.com/security-advisories/bosch-sa-454166-bt.html	H-BOS-VIDE-071122/2087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			JavaScript code which will be executed for all administrators accessing the same configuration option. **CVE ID : CVE-2022-40184**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2022	4.7	An error in the URL handler of the VIDEOJET multi 4000 may lead to a reflected cross site scripting (XSS) in the web-based interface. An attacker with knowledge of the encoder address can send a crafted link to a user, which will execute JavaScript code in the context of the user. **CVE ID : CVE-2022-40183**	https://psirt.bosch.com/security-advisories/bosch-sa-454166-bt.html	H-BOS-VIDE-071122/2088
Vendor: Cisco					
Product: meraki_mx100					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx105					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx250					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ci	H-CIS-MERA-071122/2091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**	sco-sa-meraki-mx-vpn-dos-vnESbgBf	
Product: meraki_mx400					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx450					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx600					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx64					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx64w					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx65					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx65w					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-MERA-071122/2098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**	meraki-mx-vpn-dos-vnESbgBf	
Product: meraki_mx67					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx67cw					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx67w					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx68					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx68cw					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx68w					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx75					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-MERA-071122/2105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**	meraki-mx-vpn-dos-vnESbgBf	
Product: meraki_mx84					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx85					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx95					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_vmx					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_z3					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_z3c					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	H-CIS-MERA-071122/2111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Vendor: corsair					
Product: k63					
Affected Version(s): -					
Missing Encryption of Sensitive Data	19-Oct-2022	6.8	Missing AES encryption in Corsair K63 Wireless 3.1.3 allows physically proximate attackers to inject and sniff	https://www.corsair.com/us/en/Categories/Products/Gamin	H-COR-K63-071122/2112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			keystrokes via 2.4 GHz radio transmissions. **CVE ID : CVE-2022-35860**	g-Keyboards/Wireless-Keyboards/K63-Wireless-Mechanical-Gaming-Keyboard-%E2%80%94-Blue-LED-%E2%80%94-CHERRY%C2%AE-MX-Red/p/CH-9145030-NA	
Vendor: Dlink					
Product: dir-816					
Affected Version(s): a2					
Out-of-bounds Write	26-Oct-2022	9.8	D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the srcip parameter at /goform/form2IPQoSTcAdd. **CVE ID : CVE-2022-42998**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--071122/2113
Out-of-bounds Write	26-Oct-2022	9.8	D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the wizardstep4_pskpwd parameter at /goform/form2WizardStep4. **CVE ID : CVE-2022-43000**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--071122/2114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	26-Oct-2022	9.8	D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the pskValue parameter in the setSecurity function. **CVE ID : CVE-2022-43001**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--071122/2115
Out-of-bounds Write	26-Oct-2022	9.8	D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the wizardstep54_pskpwd parameter at /goform/form2WizardStep54. **CVE ID : CVE-2022-43002**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--071122/2116
Out-of-bounds Write	26-Oct-2022	9.8	D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the pskValue parameter in the setRepeaterSecurity function. **CVE ID : CVE-2022-43003**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--071122/2117
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Oct-2022	7.5	D-Link DIR-816 A2 1.10 B05 was discovered to contain multiple command injection vulnerabilities via the admuser and admpass parameters at /goform/setSysAdm. **CVE ID : CVE-2022-42999**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--071122/2118
Product: dir-878					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Oct-2022	9.8	D-Link DIR878 1.30B08 Hotfix_04 was discovered to contain a command injection vulnerability via the component /bin/proc.cgi. **CVE ID : CVE-2022-43184**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--071122/2119
Vendor: gl-inet					
Product: gl-ax1800					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Oct-2022	8.8	gl-inet GL-MT300N-V2 Mango v3.212 and GL-AX1800 Flint v3.214 were discovered to contain multiple command injection vulnerabilities via the ping_addr and trace_addr function parameters. **CVE ID : CVE-2022-31898**	N/A	H-GL--GL-A-071122/2120
Product: gl-mt300n-v2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Oct-2022	8.8	gl-inet GL-MT300N-V2 Mango v3.212 and GL-AX1800 Flint v3.214 were discovered to contain multiple command injection vulnerabilities via the ping_addr and trace_addr function parameters. **CVE ID : CVE-2022-31898**	N/A	H-GL--GL-M-071122/2121
Vendor: Goabode					
Product: iota_all-in-one_security_kit					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.8	An os command injection vulnerability exists in the web interface util_set_abode_code functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-27804**	N/A	H-GOA-IOTA-071122/2122
Improper Access Control	25-Oct-2022	9.8	An authentication bypass vulnerability exists in the GHOME control functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted network request can lead to arbitrary XCMD execution. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-27805**	N/A	H-GOA-IOTA-071122/2123
Improper Neutralization of Special Elements used in an OS Command ('OS	25-Oct-2022	9.8	An OS command injection vulnerability exists in the web interface util_set_serial_mac functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to	N/A	H-GOA-IOTA-071122/2124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			arbitrary command execution. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-29472**		
Use of Hard-coded Credentials	25-Oct-2022	9.8	An authentication bypass vulnerability exists in the web interface /action/factory* functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP header can lead to authentication bypass. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-29477**	N/A	H-GOA-IOTA-071122/2125
Active Debug Code	25-Oct-2022	9.8	An OS command injection vulnerability exists in the console_main_loop :sys functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z. A specially-crafted XCMD can lead to arbitrary command execution. An attacker can send an XML payload to trigger this vulnerability. **CVE ID : CVE-2022-29520**	N/A	H-GOA-IOTA-071122/2126
Use of Hard-coded Credentials	25-Oct-2022	9.8	A hard-coded password vulnerability exists in the telnet functionality of Abode Systems, Inc. iota All-In-One Security Kit	N/A	H-GOA-IOTA-071122/2127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.9Z. Use of a hard-coded root password can lead to arbitrary command execution. An attacker can authenticate with hard-coded credentials to trigger this vulnerability. **CVE ID : CVE-2022-29889**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.8	An OS command injection vulnerability exists in the XCMD setUPnP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to arbitrary command execution. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-30541**	N/A	H-GOA-IOTA-071122/2128
Stack-based Buffer Overflow	25-Oct-2022	9.8	A stack-based buffer overflow vulnerability exists in the XCMD setIPCam functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to remote code execution. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-32454**	N/A	H-GOA-IOTA-071122/2129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.8	An OS command injection vulnerability exists in the XCMD doDebug functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to arbitrary command execution. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-32773**	N/A	H-GOA-IOTA-071122/2130
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.8	An OS command injection vulnerability exists in the XCMD setAlexa functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z. A specially-crafted XCMD can lead to arbitrary command execution. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-33189**	N/A	H-GOA-IOTA-071122/2131
Use of Externally-Controlled Format String	25-Oct-2022	9.8	A format string injection vulnerability exists in the ghome_process_control_packet functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted XCMD can lead to memory corruption, information disclosure and denial of service. An attacker can	N/A	H-GOA-IOTA-071122/2132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-33938**		
Use of Externally-Controlled Format String	25-Oct-2022	9.8	A format string injection vulnerability exists in the XCMD getVarHA functionality of abode systems, inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to memory corruption, information disclosure, and denial of service. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-35244**	N/A	H-GOA-IOTA-071122/2133
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	8.8	An OS command injection vulnerability exists in the web interface /action/iperf functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-30603**	N/A	H-GOA-IOTA-071122/2134
Improper Neutralization of	25-Oct-2022	8.8	An OS command injection vulnerability exists in the web	N/A	H-GOA-IOTA-071122/2135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			interface /action/ipcamRecordPost functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-32586**		
Integer Overflow or Wraparound	25-Oct-2022	8.8	An integer overflow vulnerability exists in the web interface /action/ipcamRecordPost functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to memory corruption. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-32775**	N/A	H-GOA-IOTA-071122/2136
Authentication Bypass by Capture-replay	25-Oct-2022	8.1	An information disclosure vulnerability exists in the XFINDER functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted man-in-the-middle attack can lead to increased privileges. An attacker can perform a man-in-	N/A	H-GOA-IOTA-071122/2137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the-middle attack to trigger this vulnerability. **CVE ID : CVE-2022-29475**		
Active Debug Code	25-Oct-2022	7.5	A denial of service vulnerability exists in the XCMD doDebug functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to denial of service. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-32760**	N/A	H-GOA-IOTA-071122/2138
Double Free	25-Oct-2022	6.5	A double-free vulnerability exists in the web interface /action/ipcamSetParamPost functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to memory corruption. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-32574**	N/A	H-GOA-IOTA-071122/2139
Vendor: gxgroup					
Product: gpon_ont_titanium_2122a					
Affected Version(s): c40-210					
Improper Restriction of	17-Oct-2022	9.8	An issue in GX Group GPON ONT Titanium 2122A T2122-V1.26EXL	N/A	H-GXG-GPON-071122/2140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Excessive Authentication Attempts			allows attackers to escalate privileges via a brute force attack at the login page. **CVE ID : CVE-2022-40055**		
Vendor: ip-com					
Product: ew9					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Oct-2022	9.8	IP-COM EW9 V15.11.0.14(9732) was discovered to contain a command injection vulnerability in the formSetDebugCfg function. **CVE ID : CVE-2022-43367**	N/A	H-IP--EW9-071122/2141
Exposure of Sensitive Information to an Unauthorized Actor	27-Oct-2022	7.5	IP-COM EW9 V15.11.0.14(9732) allows unauthenticated attackers to access sensitive information via the checkLoginUser, ate, telnet, version, setDebugCfg, and boot interfaces. **CVE ID : CVE-2022-43366**	N/A	H-IP--EW9-071122/2142
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	27-Oct-2022	7.5	IP-COM EW9 V15.11.0.14(9732) was discovered to contain a buffer overflow in the formSetDebugCfg function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string.	N/A	H-IP--EW9-071122/2143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43365		
N/A	27-Oct-2022	7.5	An access control issue in the password reset page of IP-COM EW9 V15.11.0.14(9732) allows unauthenticated attackers to arbitrarily change the admin password. **CVE ID : CVE-2022-43364**	N/A	H-IP--EW9-071122/2144
Vendor: iptime					
Product: nas1dual					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	17-Oct-2022	8.8	This vulnerability occurs in user accounts creation and deleteion related pages of IPTIME NAS products. The vulnerability could be exploited by a lack of validation when a POST request is made to this page. An attacker can use this vulnerability to or delete user accounts, or to escalate arbitrary user privileges. **CVE ID : CVE-2022-23771**	N/A	H-IPT-NAS1-071122/2145
Product: nas2dual					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	17-Oct-2022	8.8	This vulnerability occurs in user accounts creation and deleteion related pages of IPTIME NAS products. The vulnerability could be exploited by a lack of validation when a POST	N/A	H-IPT-NAS2-071122/2146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request is made to this page. An attacker can use this vulnerability to or delete user accounts, or to escalate arbitrary user privileges. **CVE ID : CVE-2022-23771**		
Product: nas4dual					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	17-Oct-2022	8.8	This vulnerability occurs in user accounts creation and deleteion related pages of IPTIME NAS products. The vulnerability could be exploited by a lack of validation when a POST request is made to this page. An attacker can use this vulnerability to or delete user accounts, or to escalate arbitrary user privileges. **CVE ID : CVE-2022-23771**	N/A	H-IPT-NAS4-071122/2147
Vendor: Juniper					
Product: acx7100-32c					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	5.3	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved on ACX7000 Series allows an unauthenticated network-based attacker to cause a partial Denial of Service (DoS). On	https://kb.juniper.net/JSA69878	H-JUN-ACX7-071122/2148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receipt of specific IPv6 transit traffic, Junos OS Evolved on ACX7100-48L, ACX7100-32C and ACX7509 sends this traffic to the Routing Engine (RE) instead of forwarding it, leading to increased CPU utilization of the RE and a partial DoS. This issue only affects systems configured with IPv6. This issue does not affect ACX7024 which is supported from 22.3R1-EVO onwards where the fix has already been incorporated as indicated in the solution section. This issue affects Juniper Networks Junos OS Evolved on ACX7100-48L, ACX7100-32C, ACX7509: 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S2-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2022-22227**		
Product: acx7100-48l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	5.3	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved on ACX7000 Series allows an unauthenticated network-based attacker to cause a partial Denial of Service (DoS). On receipt of specific IPv6 transit traffic, Junos OS Evolved on ACX7100-48L, ACX7100-32C and ACX7509 sends this traffic to the Routing Engine (RE) instead of forwarding it, leading to increased CPU utilization of the RE and a partial DoS. This issue only affects systems configured with IPv6. This issue does not affect ACX7024 which is supported from 22.3R1-EVO onwards where the fix has already been incorporated as indicated in the solution section. This issue affects Juniper Networks Junos OS Evolved on ACX7100-48L, ACX7100-32C, ACX7509: 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S2-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO,	https://kb.juniper.net/JSA69878	H-JUN-ACX7-071122/2149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.4R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2022-22227**		
Product: acx7509					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	5.3	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved on ACX7000 Series allows an unauthenticated network-based attacker to cause a partial Denial of Service (DoS). On receipt of specific IPv6 transit traffic, Junos OS Evolved on ACX7100-48L, ACX7100-32C and ACX7509 sends this traffic to the Routing Engine (RE) instead of forwarding it, leading to increased CPU utilization of the RE and a partial DoS. This issue only affects systems configured with IPv6. This issue does not affect ACX7024 which is supported from 22.3R1-EVO onwards where the fix has already been incorporated as indicated in the solution section. This issue affects Juniper Networks Junos	https://kb.juniper.net/JSA69878	H-JUN-ACX7-071122/2150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS Evolved on ACX7100-48L, ACX7100-32C, ACX7509: 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S2-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2022-22227**		
Product: csrx					
Affected Version(s): -					
Insufficiently Protected Credentials	18-Oct-2022	7.8	On cSRX Series devices software permission issues in the container filesystem and stored files combined with storing passwords in a recoverable format in Juniper Networks Junos OS allows a local, low-privileged attacker to elevate their permissions to take control of any instance of a cSRX software deployment. This issue affects Juniper Networks Junos OS 20.2 version 20.2R1 and later versions prior to 21.2R1 on cSRX Series. **CVE ID : CVE-2022-22251**	https://kb.juniper.net/JSA69908	H-JUN-CSRX-071122/2151
Product: ex2300					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged	https://kb.juniper.net/JSA69890	H-JUN-EX23-071122/2152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			%PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Product: ex2300-24mp					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged	https://kb.juniper.net/JSA69890	H-JUN-EX23-071122/2153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			%PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Product: ex2300-24p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged	https://kb.juniper.net/JSA69890	H-JUN-EX23-071122/2154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			%PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Product: ex2300-24t					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged	https://kb.juniper.net/JSA69890	H-JUN-EX23-071122/2155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			%PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Product: ex2300-48mp					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged	https://kb.juniper.net/JSA69890	H-JUN-EX23-071122/2156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			%PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Product: ex2300-48p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged	https://kb.juniper.net/JSA69890	H-JUN-EX23-071122/2157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			%PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Product: ex2300-48t					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged	https://kb.juniper.net/JSA69890	H-JUN-EX23-071122/2158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			%PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Product: ex2300-c					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged	https://kb.juniper.net/JSA69890	H-JUN-EX23-071122/2159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			%PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Product: ex2300m					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged	https://kb.juniper.net/JSA69890	H-JUN-EX23-071122/2160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			%PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Product: ex3400					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged	https://kb.juniper.net/JSA69890	H-JUN-EX34-071122/2161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			%PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Product: ex4300					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8,	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-24p					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-24p-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6;	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-24t					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-24t-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6;	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-32f					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-32f-dc					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6;	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-32f-s					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-48mp					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6;	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-48mp-s					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-48p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6;	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-48p-s					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-48t					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6;	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-48t-afi					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-48t-dc					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6;	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-48t-dc-afi					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-48t-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6;	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-48tafi					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-48tdc					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6;	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-48tdc-afi					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-mp					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6;	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300-vc					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4300m					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6;	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX43-071122/2184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4600					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX46-071122/2185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4600-vc					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6;	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX46-071122/2186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: ex4650					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-EX46-071122/2187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: mx10					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**	https://kb.juniper.net/JSA69892	H-JUN-MX10-071122/2188
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial	https://kb.juniper.net/JSA69906	H-JUN-MX10-071122/2189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: mx10000					
Affected Version(s): -					
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**	https://kb.juniper.net/JSA69892	H-JUN-MX10-071122/2190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions	https://kb.juniper.net/JSA69906	H-JUN-MX10-071122/2191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: mx10003					
Affected Version(s): -					
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2,	https://kb.juniper.net/JSA69892	H-JUN-MX10-071122/2192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071)	https://kb.juniper.net/JSA69906	H-JUN-MX10-071122/2193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			: EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: mx10008					
Affected Version(s): -					
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on	https://kb.juniper.net/JSA69892	H-JUN-MX10-071122/2194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(429	https://kb.juniper.net/JSA69906	H-JUN-MX10-071122/2195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: mx10016					
Affected Version(s): -					
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an	https://kb.juniper.net/JSA69892	H-JUN-MX10-071122/2196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or	https://kb.juniper.net/JSA69906	H-JUN-MX10-071122/2197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: mx104					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**	https://kb.juniper.net/JSA69892	H-JUN-MX10-071122/2198
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent	https://kb.juniper.net/JSA69906	H-JUN-MX10-071122/2199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: mx150					
Affected Version(s): -					
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1.	https://kb.juniper.net/JSA69892	H-JUN-MX15-071122/2200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22236		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-	https://kb.juniper.net/JSA69906	H-JUN-MX15-071122/2201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: mx2008					
Affected Version(s): -					
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2,	https://kb.juniper.net/JSA69892	H-JUN-MX20-071122/2202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors	https://kb.juniper.net/JSA69906	H-JUN-MX20-071122/2203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: mx2010					
Affected Version(s): -					
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This	https://kb.juniper.net/JSA69892	H-JUN-MX20-071122/2204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0]	https://kb.juniper.net/JSA69906	H-JUN-MX20-071122/2205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071): EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071): EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: mx2020					
Affected Version(s): -					
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on	https://kb.juniper.net/JSA69892	H-JUN-MX20-071122/2206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC	https://kb.juniper.net/JSA69906	H-JUN-MX20-071122/2207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22249		
Product: mx204					
Affected Version(s): -					
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**	https://kb.juniper.net/JSA69892	H-JUN-MX20-071122/2208
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding	https://kb.juniper.net/JSA69906	H-JUN-MX20-071122/2209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: mx240					
Affected Version(s): -					
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper	https://kb.juniper.net/JSA69892	H-JUN-MX24-071122/2210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series:	https://kb.juniper.net/JSA69906	H-JUN-MX24-071122/2211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: mx40					
Affected Version(s): -					
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-	https://kb.juniper.net/JSA69892	H-JUN-MX40-071122/2212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0]	https://kb.juniper.net/JSA69906	H-JUN-MX40-071122/2213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071): EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: mx480					
Affected Version(s): -					
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When	https://kb.juniper.net/JSA69892	H-JUN-MX48-071122/2214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this	https://kb.juniper.net/JSA69906	H-JUN-MX48-071122/2215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: mx5					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**	https://kb.juniper.net/JSA69892	H-JUN-MX5-071122/2216
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial	https://kb.juniper.net/JSA69906	H-JUN-MX5-071122/2217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: mx80					
Affected Version(s): -					
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**	https://kb.juniper.net/JSA69892	H-JUN-MX80-071122/2218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions	https://kb.juniper.net/JSA69906	H-JUN-MX80-071122/2219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: mx960					
Affected Version(s): -					
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2,	https://kb.juniper.net/JSA69892	H-JUN-MX96-071122/2220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071)	https://kb.juniper.net/JSA69906	H-JUN-MX96-071122/2221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			: EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Product: ptx1000					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog	https://kb.juniper.net/JSA69916	H-JUN-PTX1-071122/2222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Product: ptx1000-72q					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai"	https://kb.juniper.net/JSA69916	H-JUN-PTX1-071122/2223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Product: ptx10000					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND	https://kb.juniper.net/JSA69916	H-JUN-PTX1-071122/2224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Product: ptx10001					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a	https://kb.juniper.net/JSA69916	H-JUN-PTX1-071122/2225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22211		
Product: ptx10001-36mr					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295	https://kb.juniper.net/JSA69916	H-JUN-PTX1-071122/2226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Product: ptx100016					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space	https://kb.juniper.net/JSA69916	H-JUN-PTX1-071122/2227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Product: ptx10002					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial	https://kb.juniper.net/JSA69916	H-JUN-PTX1-071122/2228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Product: ptx10002-60c					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1	https://kb.juniper.net/JSA69916	H-JUN-PTX1-071122/2229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Product: ptx10003					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is	https://kb.juniper.net/JSA69916	H-JUN-PTX1-071122/2230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Product: ptx10003_160c					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai"	https://kb.juniper.net/JSA69916	H-JUN-PTX1-071122/2231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Product: ptx10003_80c					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND	https://kb.juniper.net/JSA69916	H-JUN-PTX1-071122/2232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Product: ptx10003_81cd					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a	https://kb.juniper.net/JSA69916	H-JUN-PTX1-071122/2233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22211		
Product: ptx10004					
Affected Version(s): -					
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Syntactic Correctness of Input vulnerability in the kernel of Juniper Networks Junos OS Evolved on PTX series allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). When an incoming TCP packet destined to the device is malformed there is a possibility of a kernel panic. Only TCP packets destined to the ports for BGP, LDP and MSDP can trigger this. This issue only affects PTX10004, PTX10008, PTX10016. No other PTX Series devices or other platforms are affected. This issue affects Juniper Networks Junos OS Evolved: 20.4-EVO versions prior to 20.4R3-S4-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 20.4R1-EVO.	https://kb.juniper.net/JSA69915	H-JUN-PTX1-071122/2234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22192		
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556	https://kb.juniper.net/JSA69916	H-JUN-PTX1-071122/2235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Product: ptx10008					
Affected Version(s): -					
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Syntactic Correctness of Input vulnerability in the kernel of Juniper Networks Junos OS Evolved on PTX series allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). When an incoming TCP packet destined to the device is malformed there is a possibility of a kernel panic. Only TCP packets destined to the ports for BGP, LDP and MSDP can trigger this. This issue only affects PTX10004, PTX10008, PTX10016. No other PTX Series devices or other platforms are affected. This issue affects Juniper Networks Junos OS Evolved: 20.4-EVO	https://kb.juniper.net/JSA69915	H-JUN-PTX1-071122/2236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.4R3-S4-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 20.4R1-EVO. **CVE ID : CVE-2022-22192**		
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295	https://kb.juniper.net/JSA69916	H-JUN-PTX1-071122/2237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Product: ptx10016					
Affected Version(s): -					
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Syntactic Correctness of Input vulnerability in the kernel of Juniper Networks Junos OS Evolved on PTX series allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). When an incoming TCP packet destined to the device is malformed there is a possibility of a kernel	https://kb.juniper.net/JSA69915	H-JUN-PTX1-071122/2238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			panic. Only TCP packets destined to the ports for BGP, LDP and MSDP can trigger this. This issue only affects PTX10004, PTX10008, PTX10016. No other PTX Series devices or other platforms are affected. This issue affects Juniper Networks Junos OS Evolved: 20.4-EVO versions prior to 20.4R3-S4-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 20.4R1-EVO. **CVE ID : CVE-2022-22192**		
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-	https://kb.juniper.net/JSA69916	H-JUN-PTX1-071122/2239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			%USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Product: ptx3000					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai"	https://kb.juniper.net/JSA69916	H-JUN-PTX3-071122/2240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Product: ptx5000					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND	https://kb.juniper.net/JSA69916	H-JUN-PTX5-071122/2241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Product: qfx10002					
Affected Version(s): -					
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows	https://kb.juniper.net/JSA69873	H-JUN-QFX1-071122/2242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more and reviewing for backpressured output; for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qfx10008					
Affected Version(s): -					
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All	https://kb.juniper.net/JSA69873	H-JUN-QFX1-071122/2243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more and reviewing for backpressured output; for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		
Product: qfx10016					
Affected Version(s): -					
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be	https://kb.juniper.net/JSA69873	H-JUN-QFX1-071122/2244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			destined to the device or be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more and reviewing for backpressured output; for example: GOT:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		
Product: qfx5100					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.ht	H-JUN-QFX5-071122/2245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This	ml#id-vxlan__d281e31	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: qfx5110					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-QFX5-071122/2246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: qfx5120					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-	H-JUN-QFX5-071122/2247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect	vxlan__d281e31	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: qfx5130					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-QFX5-071122/2248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: qfx5200					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-	H-JUN-QFX5-071122/2249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1.	vxlan__d281e31	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22226		
Product: qfx5210					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-QFX5-071122/2250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: qfx5220					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device.	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-QFX5-071122/2251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22226		
Product: qfx5700					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	H-JUN-QFX5-071122/2252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Product: srx100					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server,	https://kb.juniper.net/JSA69901	H-JUN-SRX1-071122/2253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-	https://kb.juniper.net/JSA69886	H-JUN-SRX1-071122/2254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to	https://kb.juniper.net/JSA69891	H-JUN-SRX1-071122/2255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does	https://kb.juniper.net/JSA69892	H-JUN-SRX1-071122/2256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx110					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions	https://kb.juniper.net/JSA69901	H-JUN-SRX1-071122/2257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**	https://kb.juniper.net/JSA69886	H-JUN-SRX1-071122/2258
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker	https://kb.juniper.net/JSA69891	H-JUN-SRX1-071122/2259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer	https://kb.juniper.net/JSA69892	H-JUN-SRX1-071122/2260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx1400					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of	https://kb.juniper.net/JSA69901	H-JUN-SRX1-071122/2261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content	https://kb.juniper.net/JSA69886	H-JUN-SRX1-071122/2262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address	https://kb.juniper.net/JSA69891	H-JUN-SRX1-071122/2263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to	https://kb.juniper.net/JSA69892	H-JUN-SRX1-071122/2264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx1500					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2	https://kb.juniper.net/JSA69901	H-JUN-SRX1-071122/2265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	An Unchecked Return Value to NULL Pointer Dereference vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series if Unified Threat Management (UTM) Enhanced Content Filtering (CF) and AntiVirus (AV) are enabled together and the system processes specific valid transit traffic the Packet Forwarding Engine (PFE) will crash and restart. This issue affects Juniper Networks Junos OS 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22231**	https://kb.juniper.net/JSA69885	H-JUN-SRX1-071122/2266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**	https://kb.juniper.net/JSA69886	H-JUN-SRX1-071122/2267
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP)	https://kb.juniper.net/JSA69891	H-JUN-SRX1-071122/2268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an	https://kb.juniper.net/JSA69892	H-JUN-SRX1-071122/2269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx210					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an	https://kb.juniper.net/JSA69901	H-JUN-SRX2-071122/2270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This	https://kb.juniper.net/JSA69886	H-JUN-SRX2-071122/2271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions	https://kb.juniper.net/JSA69891	H-JUN-SRX2-071122/2272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2,	https://kb.juniper.net/JSA69892	H-JUN-SRX2-071122/2273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx220					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1	https://kb.juniper.net/JSA69901	H-JUN-SRX2-071122/2274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**	https://kb.juniper.net/JSA69886	H-JUN-SRX2-071122/2275
Improper Check for Unusual or Exceptional	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on	https://kb.juniper.net/JSA69891	H-JUN-SRX2-071122/2276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conditions			SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**	https://kb.juniper.net/JSA69892	H-JUN-SRX2-071122/2277
Product: srx240					
Affected Version(s): -					
Improper Check for Unusual or Exceptional	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-	https://kb.juniper.net/JSA69901	H-JUN-SRX2-071122/2278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conditions			enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of	https://kb.juniper.net/JSA69886	H-JUN-SRX2-071122/2279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue	https://kb.juniper.net/JSA69891	H-JUN-SRX2-071122/2280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX	https://kb.juniper.net/JSA69892	H-JUN-SRX2-071122/2281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx240h2					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2	https://kb.juniper.net/JSA69901	H-JUN-SRX2-071122/2282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1.	https://kb.juniper.net/JSA69886	H-JUN-SRX2-071122/2283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22232		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1,	https://kb.juniper.net/JSA69891	H-JUN-SRX2-071122/2284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**	https://kb.juniper.net/JSA69892	H-JUN-SRX2-071122/2285
Product: srx240m					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**	https://kb.juniper.net/JSA69901	H-JUN-SRX2-071122/2286
NULL Pointer	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the	https://kb.juniper.net/JSA69886	H-JUN-SRX2-071122/2287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP	https://kb.juniper.net/JSA69891	H-JUN-SRX2-071122/2288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of	https://kb.juniper.net/JSA69892	H-JUN-SRX2-071122/2289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx300					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server,	https://kb.juniper.net/JSA69901	H-JUN-SRX3-071122/2290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-	https://kb.juniper.net/JSA69886	H-JUN-SRX3-071122/2291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to	https://kb.juniper.net/JSA69891	H-JUN-SRX3-071122/2292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does	https://kb.juniper.net/JSA69892	H-JUN-SRX3-071122/2293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx320					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions	https://kb.juniper.net/JSA69901	H-JUN-SRX3-071122/2294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**	https://kb.juniper.net/JSA69886	H-JUN-SRX3-071122/2295
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker	https://kb.juniper.net/JSA69891	H-JUN-SRX3-071122/2296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer	https://kb.juniper.net/JSA69892	H-JUN-SRX3-071122/2297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx340					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of	https://kb.juniper.net/JSA69901	H-JUN-SRX3-071122/2298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content	https://kb.juniper.net/JSA69886	H-JUN-SRX3-071122/2299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address	https://kb.juniper.net/JSA69891	H-JUN-SRX3-071122/2300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to	https://kb.juniper.net/JSA69892	H-JUN-SRX3-071122/2301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx3400					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2	https://kb.juniper.net/JSA69901	H-JUN-SRX3-071122/2302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**	https://kb.juniper.net/JSA69886	H-JUN-SRX3-071122/2303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper	https://kb.juniper.net/JSA69891	H-JUN-SRX3-071122/2304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**	https://kb.juniper.net/JSA69892	H-JUN-SRX3-071122/2305
Product: srx345					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**	https://kb.juniper.net/JSA69901	H-JUN-SRX3-071122/2306
NULL Pointer	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the	https://kb.juniper.net/JSA69886	H-JUN-SRX3-071122/2307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP	https://kb.juniper.net/JSA69891	H-JUN-SRX3-071122/2308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of	https://kb.juniper.net/JSA69892	H-JUN-SRX3-071122/2309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx3600					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server,	https://kb.juniper.net/JSA69901	H-JUN-SRX3-071122/2310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-	https://kb.juniper.net/JSA69886	H-JUN-SRX3-071122/2311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to	https://kb.juniper.net/JSA69891	H-JUN-SRX3-071122/2312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does	https://kb.juniper.net/JSA69892	H-JUN-SRX3-071122/2313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx380					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions	https://kb.juniper.net/JSA69901	H-JUN-SRX3-071122/2314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**	https://kb.juniper.net/JSA69886	H-JUN-SRX3-071122/2315
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker	https://kb.juniper.net/JSA69891	H-JUN-SRX3-071122/2316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer	https://kb.juniper.net/JSA69892	H-JUN-SRX3-071122/2317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx4000					
Affected Version(s): -					
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of	https://kb.juniper.net/JSA69900	H-JUN-SRX4-071122/2318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid	https://kb.juniper.net/JSA69901	H-JUN-SRX4-071122/2319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will	https://kb.juniper.net/JSA69886	H-JUN-SRX4-071122/2320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on	https://kb.juniper.net/JSA69891	H-JUN-SRX4-071122/2321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions	https://kb.juniper.net/JSA69892	H-JUN-SRX4-071122/2322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx4100					
Affected Version(s): -					
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions	https://kb.juniper.net/JSA69900	H-JUN-SRX4-071122/2323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to	https://kb.juniper.net/JSA69901	H-JUN-SRX4-071122/2324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	An Unchecked Return Value to NULL Pointer Dereference vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series if Unified Threat Management (UTM) Enhanced Content Filtering (CF) and AntiVirus (AV) are enabled together and the system processes specific valid transit traffic the Packet Forwarding Engine (PFE) will crash and restart. This issue affects Juniper Networks Junos OS 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22231**	https://kb.juniper.net/JSA69885	H-JUN-SRX4-071122/2325
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on	https://kb.juniper.net/JSA69886	H-JUN-SRX4-071122/2326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The	https://kb.juniper.net/JSA69891	H-JUN-SRX4-071122/2327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will	https://kb.juniper.net/JSA69892	H-JUN-SRX4-071122/2328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx4200					
Affected Version(s): -					
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This	https://kb.juniper.net/JSA69900	H-JUN-SRX4-071122/2329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions	https://kb.juniper.net/JSA69901	H-JUN-SRX4-071122/2330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	An Unchecked Return Value to NULL Pointer Dereference vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series if Unified Threat Management (UTM) Enhanced Content Filtering (CF) and AntiVirus (AV) are enabled together and the system processes specific valid transit traffic the Packet Forwarding Engine (PFE) will crash and restart. This issue affects Juniper Networks Junos OS 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series. This issue does not affect	https://kb.juniper.net/JSA69885	H-JUN-SRX4-071122/2331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22231**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**	https://kb.juniper.net/JSA69886	H-JUN-SRX4-071122/2332
Improper Check for Unusual or Exceptional	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated,	https://kb.juniper.net/JSA69891	H-JUN-SRX4-071122/2333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conditions			network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitiali	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP	https://kb.juniper.net/JSA69892	H-JUN-SRX4-071122/2334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
zed Pointer			Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx4600					
Affected Version(s): -					
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker	https://kb.juniper.net/JSA69900	H-JUN-SRX4-071122/2335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid	https://kb.juniper.net/JSA69901	H-JUN-SRX4-071122/2336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	An Unchecked Return Value to NULL Pointer Dereference vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series if Unified Threat Management (UTM) Enhanced Content Filtering (CF) and AntiVirus (AV) are	https://kb.juniper.net/JSA69885	H-JUN-SRX4-071122/2337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabled together and the system processes specific valid transit traffic the Packet Forwarding Engine (PFE) will crash and restart. This issue affects Juniper Networks Junos OS 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22231**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper	https://kb.juniper.net/JSA69886	H-JUN-SRX4-071122/2338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions	https://kb.juniper.net/JSA69891	H-JUN-SRX4-071122/2339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**	https://kb.juniper.net/JSA69892	H-JUN-SRX4-071122/2340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: srx5000					
Affected Version(s): -					
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**	https://kb.juniper.net/JSA69900	H-JUN-SRX5-071122/2341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**	https://kb.juniper.net/JSA69901	H-JUN-SRX5-071122/2342
NULL Pointer	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the	https://kb.juniper.net/JSA69886	H-JUN-SRX5-071122/2343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP	https://kb.juniper.net/JSA69891	H-JUN-SRX5-071122/2344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of	https://kb.juniper.net/JSA69892	H-JUN-SRX5-071122/2345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx5400					
Affected Version(s): -					
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet	https://kb.juniper.net/JSA69900	H-JUN-SRX5-071122/2346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This	https://kb.juniper.net/JSA69901	H-JUN-SRX5-071122/2347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	An Unchecked Return Value to NULL Pointer Dereference vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series if Unified Threat Management (UTM) Enhanced Content Filtering (CF) and AntiVirus (AV) are enabled together and the system processes specific valid transit traffic the Packet Forwarding Engine (PFE) will crash and restart. This issue affects Juniper Networks Junos OS 21.4 versions	https://kb.juniper.net/JSA69885	H-JUN-SRX5-071122/2348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.4R1-S2, 21.4R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22231**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**	https://kb.juniper.net/JSA69886	H-JUN-SRX5-071122/2349
Improper Check for Unusual or Exception	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper	https://kb.juniper.net/JSA69891	H-JUN-SRX5-071122/2350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
al Conditions			Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**	https://kb.juniper.net/JSA69892	H-JUN-SRX5-071122/2351
Product: srx550					
Affected Version(s): -					
Improper Check for Unusual or Exceptional	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-	https://kb.juniper.net/JSA69901	H-JUN-SRX5-071122/2352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conditions			enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	An Unchecked Return Value to NULL Pointer Dereference vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause a Denial of	https://kb.juniper.net/JSA69885	H-JUN-SRX5-071122/2353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS). On SRX Series if Unified Threat Management (UTM) Enhanced Content Filtering (CF) and AntiVirus (AV) are enabled together and the system processes specific valid transit traffic the Packet Forwarding Engine (PFE) will crash and restart. This issue affects Juniper Networks Junos OS 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22231**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-	https://kb.juniper.net/JSA69886	H-JUN-SRX5-071122/2354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to	https://kb.juniper.net/JSA69891	H-JUN-SRX5-071122/2355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does	https://kb.juniper.net/JSA69892	H-JUN-SRX5-071122/2356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx550m					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions	https://kb.juniper.net/JSA69901	H-JUN-SRX5-071122/2357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**	https://kb.juniper.net/JSA69886	H-JUN-SRX5-071122/2358
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker	https://kb.juniper.net/JSA69891	H-JUN-SRX5-071122/2359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer	https://kb.juniper.net/JSA69892	H-JUN-SRX5-071122/2360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx550_hm					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of	https://kb.juniper.net/JSA69901	H-JUN-SRX5-071122/2361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content	https://kb.juniper.net/JSA69886	H-JUN-SRX5-071122/2362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address	https://kb.juniper.net/JSA69891	H-JUN-SRX5-071122/2363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to	https://kb.juniper.net/JSA69892	H-JUN-SRX5-071122/2364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx5600					
Affected Version(s): -					
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2	https://kb.juniper.net/JSA69900	H-JUN-SRX5-071122/2365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions	https://kb.juniper.net/JSA69901	H-JUN-SRX5-071122/2366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	An Unchecked Return Value to NULL Pointer Dereference vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series if Unified Threat Management (UTM) Enhanced Content Filtering (CF) and AntiVirus (AV) are enabled together and the system processes specific valid transit traffic the Packet Forwarding Engine (PFE) will crash and restart. This issue affects Juniper Networks Junos OS 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22231**	https://kb.juniper.net/JSA69885	H-JUN-SRX5-071122/2367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**	https://kb.juniper.net/JSA69886	H-JUN-SRX5-071122/2368
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP)	https://kb.juniper.net/JSA69891	H-JUN-SRX5-071122/2369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an	https://kb.juniper.net/JSA69892	H-JUN-SRX5-071122/2370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: srx5800					
Affected Version(s): -					
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when	https://kb.juniper.net/JSA69900	H-JUN-SRX5-071122/2371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PowerMode IPsec is configured and a malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server,	https://kb.juniper.net/JSA69901	H-JUN-SRX5-071122/2372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
NULL Pointer Dereference	18-Oct-2022	7.5	An Unchecked Return Value to NULL Pointer Dereference vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series if Unified Threat Management (UTM) Enhanced Content Filtering (CF) and AntiVirus (AV) are enabled together and the system processes specific valid transit traffic the Packet Forwarding Engine (PFE) will crash	https://kb.juniper.net/JSA69885	H-JUN-SRX5-071122/2373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and restart. This issue affects Juniper Networks Junos OS 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22231**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**	https://kb.juniper.net/JSA69886	H-JUN-SRX5-071122/2374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper	https://kb.juniper.net/JSA69891	H-JUN-SRX5-071122/2375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**	https://kb.juniper.net/JSA69892	H-JUN-SRX5-071122/2376
Product: srx650					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**	https://kb.juniper.net/JSA69901	H-JUN-SRX6-071122/2377
NULL Pointer	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the	https://kb.juniper.net/JSA69886	H-JUN-SRX6-071122/2378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP	https://kb.juniper.net/JSA69891	H-JUN-SRX6-071122/2379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of	https://kb.juniper.net/JSA69892	H-JUN-SRX6-071122/2380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Product: vsrx					
Affected Version(s): -					
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet	https://kb.juniper.net/JSA69900	H-JUN-VSRX-071122/2381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**		
Vendor: lannerinc					
Product: iac-ast2500					
Affected Version(s): -					
Use of Hard-coded Credentials	24-Oct-2022	8.1	Use of hard-coded TLS certificate by default allows an attacker to perform Man-in-the-Middle (MitM) attacks even in the presence of the HTTPS connection. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.00.0. **CVE ID : CVE-2021-4228**	N/A	H-LAN-IAC--071122/2382
Product: iac-ast2500a					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Session Expiration	24-Oct-2022	9.8	Session fixation and insufficient session expiration vulnerabilities allow an attacker to perfom session hijacking attacks against users. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-46279**	N/A	H-LAN-IAC--071122/2383
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Oct-2022	9.8	Command injection and multiple stack-based buffer overflows vulnerabilities in the modifyUserb_func function of spx_restservice allow an attacker to execute arbitrary code with the same privileges as the server user (root). This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-26731**	N/A	H-LAN-IAC--071122/2384
Out-of-bounds Write	24-Oct-2022	9.8	A stack-based buffer overflow vulnerability in a subfunction of the Login_handler_func function of spx_restservice allows an attacker to execute arbitrary code with the same privileges as the server user (root). This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0.	N/A	H-LAN-IAC--071122/2385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26730		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Oct-2022	9.8	Command injection and multiple stack-based buffer overflows vulnerabilities in the Login_handler_func function of spx_restservice allow an attacker to execute arbitrary code with the same privileges as the server user (root). This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-26729**	N/A	H-LAN-IAC--071122/2386
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Oct-2022	9.8	Command injection and stack-based buffer overflow vulnerabilities in the KillDupUsr_func function of spx_restservice allow an attacker to execute arbitrary code with the same privileges as the server user (root). This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-26728**	N/A	H-LAN-IAC--071122/2387
Improper Neutralization of Special Elements used in a Command ('Comma	24-Oct-2022	9.8	Multiple command injections and stack-based buffer overflows vulnerabilities in the SubNet_handler_func function of spx_restservice allow an attacker to execute arbitrary code with the	N/A	H-LAN-IAC--071122/2388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
nd Injection')			same privileges as the server user (root). This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-26727**		
Improper Input Validation	24-Oct-2022	7.5	An improper input validation vulnerability in the TLS certificate generation function allows an attacker to cause a Denial-of-Service (DoS) condition which can only be reverted via a factory reset. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-44769**	N/A	H-LAN-IAC--071122/2389
N/A	24-Oct-2022	7.5	A broken access control vulnerability in the KillDupUsr_func function of spx_restservice allows an attacker to arbitrarily terminate active sessions of other users, causing a Denial-of-Service (DoS) condition. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-44467**	N/A	H-LAN-IAC--071122/2390
Missing Authorization	24-Oct-2022	7.5	A broken access control vulnerability in the FirstReset_handler_func function of spx_restservice allows an attacker to arbitrarily send reboot commands	N/A	H-LAN-IAC--071122/2391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the BMC, causing a Denial-of-Service (DoS) condition. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-26733**		
Observable Discrepancy	24-Oct-2022	5.3	Observable discrepancies in the login process allow an attacker to guess legitimate user names registered in the BMC. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-45925**	N/A	H-LAN-IAC--071122/2392
Missing Authorization	24-Oct-2022	5.3	A broken access control vulnerability in the SubNet_handler_func function of spx_restservice allows an attacker to arbitrarily change the security access rights to KVM and Virtual Media functionalities. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-44776**	N/A	H-LAN-IAC--071122/2393
Missing Authorization	24-Oct-2022	5.3	A broken access control vulnerability in the First_network_func function of spx_restservice allows an attacker to arbitrarily change the network configuration of the BMC.	N/A	H-LAN-IAC--071122/2394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-26732**		
Vendor: Netgear					
Product: r6220					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Oct-2022	8.8	Netgear R6220 v1.1.0.114_1.0.1 suffers from Incorrect Access Control, resulting in a command injection vulnerability. **CVE ID : CVE-2022-42221**	https://www.netgear.com/about/security/	H-NET-R622-071122/2395
Vendor: oringnet					
Product: iap-420					
Affected Version(s): -					
Hidden Functionality	21-Oct-2022	8.8	On ORing net IAP-420(+) with FW version 2.0m a telnet server is enabled by default and cannot permanently be disabled. You can connect to the device with with hardcoded credentials and get an administrative shell. These credentials are reset to defaults with every reboot. **CVE ID : CVE-2022-3203**	https://mads.uniud.it/2022/09/lord-of-the-orings/	H-ORI-IAP--071122/2396
Product: iap-420\+					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Hidden Functionality	21-Oct-2022	8.8	On ORing net IAP-420(+) with FW version 2.0m a telnet server is enabled by default and cannot permanently be disabled. You can connect to the device with with hardcoded credentials and get an administrative shell. These credentials are reset to defaults with every reboot. **CVE ID : CVE-2022-3203**	https://mads.uniud.it/2022/09/lord-of-the-orings/	H-ORI-IAP--071122/2397
Vendor: Qualcomm					
Product: apq8009					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2398
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2400
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2402
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-APQ8-071122/2403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2404
Product: apq8009w					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2406
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2408
Product: apq8016					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2410
Product: apq8017					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2412
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2414
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2416
Product: apq8037					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2418
Product: apq8052					
Affected Version(s): -					
Buffer Copy without Checking	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-APQ8-071122/2419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2420
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2422
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: apq8053					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2424
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2426
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2428
Product: apq8056					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2429
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication	https://www.qualcomm.com/company/product-	H-QUA-APQ8-071122/2430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2431
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-APQ8-071122/2432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	r-2022-bulletin	
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2433
Product: apq8064au					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2435
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2437
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2438
Product: apq8076					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2439
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2440
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-APQ8-071122/2441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2442
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-APQ8-071122/2443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2444
Exposure of Sensitive Informati	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in	https://www.qualcomm.com/company/product-	H-QUA-APQ8-071122/2445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on to an Unauthorized Actor			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	security/bulletins/october-2022-bulletin	
Product: apq8084					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2446
Product: apq8092					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value	https://www.qualcomm.com/compa	H-QUA-APQ8-071122/2447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	ny/product-security/bulletins/october-2022-bulletin	
Product: apq8094					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Product: apq8096au					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2449
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2451
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2453
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2454
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2456
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-APQ8-071122/2457
Product: aqt1000					
Affected Version(s): -					
Buffer Copy without Checking	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-AQT1-071122/2458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AQT1-071122/2459
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AQT1-071122/2460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AQT1-071122/2461
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AQT1-071122/2462
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AQT1-071122/2463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AQT1-071122/2464
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AQT1-071122/2465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25665		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AQT1-071122/2466
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AQT1-071122/2467
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AQT1-071122/2468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25663		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AQT1-071122/2469
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AQT1-071122/2470
Product: ar6003					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-AR60-071122/2471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Product: ar8031					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR80-071122/2472
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR80-071122/2473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR80-071122/2474
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR80-071122/2475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR80-071122/2476
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR80-071122/2477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR80-071122/2478
Product: ar8035					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-AR80-071122/2479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR80-071122/2480
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-AR80-071122/2481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR80-071122/2482
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR80-071122/2483
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-AR80-071122/2484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR80-071122/2485
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR80-071122/2486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22078		
Product: ar9380					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR93-071122/2487
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR93-071122/2488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR93-071122/2489
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-AR93-071122/2490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: csr8811					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSR8-071122/2491
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSR8-071122/2492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSR8-071122/2493
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSR8-071122/2494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSR8-071122/2495
Product: csra6620					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRA-071122/2496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRA-071122/2497
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRA-071122/2498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRA-071122/2499
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRA-071122/2500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRA-071122/2501
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRA-071122/2502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: csra6640					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRA-071122/2503
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRA-071122/2504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRA-071122/2505
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRA-071122/2506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRA-071122/2507
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRA-071122/2508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRA-071122/2509
Product: csrb31024					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRB-071122/2510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRB-071122/2511
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRB-071122/2512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRB-071122/2513
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRB-071122/2514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-CSRB-071122/2515
Product: fsm10056					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-FSM1-071122/2516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-FSM1-071122/2517
Product: ipq4018					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ4-071122/2518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ4-071122/2519
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ4-071122/2520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ4-071122/2521
Product: ipq4019					
Affected Version(s): -					
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ4-071122/2522
Product: ipq4028					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ4-071122/2523
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ4-071122/2524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ4-071122/2525
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ4-071122/2526
Product: ipq4029					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ4-071122/2527
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ4-071122/2528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ4-071122/2529
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ4-071122/2530
Product: ipq5010					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ5-071122/2531
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ5-071122/2532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ5-071122/2533
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ5-071122/2534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ5-071122/2535
Product: ipq5018					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ5-071122/2536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ5-071122/2537
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ5-071122/2538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ5-071122/2539
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ5-071122/2540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Product: ipq5028					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ5-071122/2541
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ5-071122/2542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ5-071122/2543
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ5-071122/2544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ5-071122/2545
Product: ipq6000					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ6-071122/2546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ6-071122/2547
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ6-071122/2548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ6-071122/2549
Product: ipq6010					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ6-071122/2550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ6-071122/2551
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ6-071122/2552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ6-071122/2553
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different	https://www.qualcomm.com/company/product-	H-QUA-IPQ6-071122/2554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	security/bulletins/october-2022-bulletin	
Product: ipq6018					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ6-071122/2555
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ6-071122/2556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ6-071122/2557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ6-071122/2558
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ6-071122/2559
Product: ipq6028					
Affected Version(s): -					
Integer Overflow	19-Oct-2022	9.8	Memory corruption in WLAN due to integer	https://www.qualcomm	H-QUA-IPQ6-071122/2560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ6-071122/2561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25719		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ6-071122/2562
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ6-071122/2563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ6-071122/2564
Product: ipq8064					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2566
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2568
Product: ipq8065					
Affected Version(s): -					
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2569
Product: ipq8068					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2570
Product: ipq8069					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2572
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Product: ipq8070					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2574
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2576
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: ipq8070a					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2578
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2580
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2582
Product: ipq8071					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2584
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: ipq8071a					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2586
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-IPQ8-071122/2587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2588
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-071122/2589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2590
Product: ipq8072					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-IPQ8-071122/2591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2592
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-071122/2593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	security/bulletins/october-2022-bulletin	
Product: ipq8072a					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2595
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2597
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq8074					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2599
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2601
Product: ipq8074a					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2603
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2605
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: ipq8076					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2607
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2609
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2611
Product: ipq8076a					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2613
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-IPQ8-071122/2614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2615
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-IPQ8-071122/2616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Product: ipq8078					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2617
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2619
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-IPQ8-071122/2620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2621
Product: ipq8078a					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2623
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ8-071122/2624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2625
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-071122/2626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	security/bulletins/october-2022-bulletin	
Product: ipq8173					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2627
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ8-071122/2628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2630
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2631
Product: ipq8174					
Affected Version(s): -					
Integer Overflow	19-Oct-2022	9.8	Memory corruption in WLAN due to integer	https://www.qualcomm	H-QUA-IPQ8-071122/2632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25719		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2634
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ8-071122/2636
Product: ipq9008					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ9-071122/2637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ9-071122/2638
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-IPQ9-071122/2639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: kailua					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-KAIL-071122/2640
Product: mdm8215					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM8-071122/2641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM8-071122/2642
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM8-071122/2643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM8-071122/2644
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM8-071122/2645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Product: mdm8215m					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM8-071122/2646
Product: mdm8615m					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM8-071122/2647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Product: mdm9150					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2648
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2650
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2651
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: mdm9205					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2653
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: mdm9206					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2655
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2657
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2659
Product: mdm9215					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2661
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2663
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: mdm9225					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2665
Product: mdm9225m					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while	https://www.qualcomm.com/compa	H-QUA-MDM9-071122/2666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	ny/product-security/bulletins/october-2022-bulletin	
Product: mdm9230					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2668
Product: mdm9235m					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: mdm9250					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2670
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2672
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2674
Product: mdm9310					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2676
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2678
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: mdm9330					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2680
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: mdm9607					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2682
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2684
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2686
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: mdm9615					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2688
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2690
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2692
Product: mdm9615m					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-MDM9-071122/2693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Product: mdm9625					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2694
Product: mdm9625m					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2695
Product: mdm9628					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2697
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2699
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2701
Product: mdm9630					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2703
Product: mdm9635m					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: mdm9640					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2705
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2707
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: mdm9645					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2709
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in	https://www.qualcomm.com/company/product-security/bull	H-QUA-MDM9-071122/2710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2711
Product: mdm9650					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2712
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2713
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-MDM9-071122/2714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2715
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-MDM9-071122/2716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2717
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MDM9-071122/2718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: msm8108					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2719
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2721
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25719		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2723
Product: msm8208					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2724
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-MSM8-071122/2725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2726
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2728
Product: msm8209					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2730
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2732
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: msm8608					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2734
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2735
Improper Validation	19-Oct-2022	9.8	Memory corruption in WLAN due to out of	https://www.qualcomm	H-QUA-MSM8-071122/2736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2737
Exposure of Sensitive	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU	https://www.qualcomm.com/compa	H-QUA-MSM8-071122/2738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information to an Unauthorized Actor			reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	ny/product-security/bulletins/october-2022-bulletin	
Product: msm8909w					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2739
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2741
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: msm8917					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2743
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2745
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: msm8920					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2747
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: msm8937					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2749
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-MSM8-071122/2750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	r-2022-bulletin	
Product: msm8940					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2752
Product: msm8952					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2754
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2756
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2757
Product: msm8953					
Affected Version(s): -					
Buffer Copy	19-Oct-2022	9.8	memory corruption in video due to buffer	https://www.qualcomm	H-QUA-MSM8-071122/2758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	.com/company/product-security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2759
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-MSM8-071122/2760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2761
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-MSM8-071122/2762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	r-2022-bulletin	
Product: msm8956					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2763
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2765
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2767
Product: msm8976					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2768
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication	https://www.qualcomm.com/company/product-	H-QUA-MSM8-071122/2769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2770
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-MSM8-071122/2771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2773
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2774
Product: msm8976sg					
Affected Version(s): -					
Buffer Copy without	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing	https://www.qualcomm.com/compa	H-QUA-MSM8-071122/2775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	ny/product-security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2776
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-MSM8-071122/2777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2778
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: msm8992					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2780
Product: msm8994					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Product: msm8996au					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2782
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2784
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2786
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2787
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2789
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-MSM8-071122/2790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: pm8937					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-PM89-071122/2791
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-PM89-071122/2792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: pmp8074					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-PMP8-071122/2793
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-PMP8-071122/2794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-PMP8-071122/2795
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-PMP8-071122/2796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Product: qam8295p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QAM8-071122/2797
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QAM8-071122/2798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QAM8-071122/2799
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QAM8-071122/2800
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QAM8-071122/2801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	etins/october-2022-bulletin	
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QAM8-071122/2802
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QAM8-071122/2803
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QAM8-071122/2804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QAM8-071122/2805
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QAM8-071122/2806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QAM8-071122/2807
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QAM8-071122/2808
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QAM8-071122/2809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25664		
Product: qca0000					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA0-071122/2810
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA0-071122/2811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qca1023					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA1-071122/2812
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA1-071122/2813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA1-071122/2814
Product: qca1062					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA1-071122/2815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA1-071122/2816
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA1-071122/2817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA1-071122/2818
Product: qca1064					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA1-071122/2819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA1-071122/2820
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA1-071122/2821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA1-071122/2822
Product: qca1990					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA1-071122/2823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA1-071122/2824
Product: qca2062					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA2-071122/2825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA2-071122/2826
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA2-071122/2827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA2-071122/2828
Product: qca2064					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA2-071122/2829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA2-071122/2830
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA2-071122/2831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA2-071122/2832
Product: qca2065					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA2-071122/2833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA2-071122/2834
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA2-071122/2835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA2-071122/2836
Product: qca2066					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA2-071122/2837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA2-071122/2838
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA2-071122/2839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA2-071122/2840
Product: qca4004					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2842
Product: qca4010					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2844
Product: qca4020					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2846
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2848
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2850
Product: qca4024					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2852
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2854
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA4-071122/2855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2856
Product: qca4531					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA4-071122/2858
Product: qca6164					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing	https://www.qualcomm.com/company/product-	H-QUA-QCA6-071122/2859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	security/bulletins/october-2022-bulletin	
Product: qca6174					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2861
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2863
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qca6174a					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2865
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2867
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2869
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2870
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/2871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2872
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2874
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2875
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: qca6175a					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2877
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2879
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qca6310					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2881
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2883
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2885
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2886
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2888
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2890
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2891
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2893
Product: qca6320					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2894
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/2895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2896
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2898
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2900
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2902
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2903
Product: qca6335					
Affected Version(s): -					
Buffer Copy without	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing	https://www.qualcomm.com/compa	H-QUA-QCA6-071122/2904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	ny/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2905
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2907
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2908
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2910
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2912
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2913
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2915
Product: qca6390					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2916
Improper Validation	19-Oct-2022	9.8	Memory corruption in WLAN due to out of	https://www.qualcomm	H-QUA-QCA6-071122/2917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	.com/company/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2918
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon	https://www.qualcomm.com/compa	H-QUA-QCA6-071122/2919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	ny/product-security/bulletins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2920
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2921
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2923
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25665		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2925
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2926
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25663		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2928
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2929
Product: qca6391					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/2930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2931
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2933
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2934
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25662		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2936
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2938
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2939
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2941
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2942
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: qca6420					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2944
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2946
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2947
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25661		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2949
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2951
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2952
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2954
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2955
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: qca6421					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2957
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2959
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2960
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25661		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2962
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2963
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in	https://www.qualcomm.com/company/product-	H-QUA-QCA6-071122/2964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2965
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2967
Product: qca6426					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2968
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/2969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2970
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/2971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2972
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2973
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2975
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2976
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in	https://www.qualcomm	H-QUA-QCA6-071122/2977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	.com/company/product-security/bulletins/october-2022-bulletin	
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2978
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: qca6428					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2980
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2982
Product: qca6430					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2984
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2986
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2987
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2989
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2990
Time-of-check Time-of-use	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size	https://www.qualcomm.com/company/product-	H-QUA-QCA6-071122/2991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2992
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2993
Exposure of Sensitive Information to an	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-071122/2994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2995
Product: qca6431					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2997
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/2999
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3000
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3002
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3004
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3005
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22078		
Product: qca6436					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3007
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3008
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer	https://www.qualcomm.com/compa	H-QUA-QCA6-071122/3009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	ny/product-security/bulletins/october-2022-bulletin	
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3010
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3012
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3013
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/3014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3015
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3016
Exposure of	19-Oct-2022	5.5	Information disclosure due to exposure of	https://www.qualcomm	H-QUA-QCA6-071122/3017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information to an Unauthorized Actor			information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	.com/company/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3018
Product: qca6438					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3020
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/3021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Product: qca6554a					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3022
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming	https://www.qualcomm.com/company/product-	H-QUA-QCA6-071122/3023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3024
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-071122/3025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3026
Product: qca6564					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3027
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3028
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-071122/3029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3030
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/3031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3032
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3034
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3035
Product: qca6564a					
Affected Version(s): -					
Buffer Copy without	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing	https://www.qualcomm.com/compa	H-QUA-QCA6-071122/3036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	ny/product-security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3037
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/3038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3039
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25660		
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3041
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3042
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3043
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-071122/3044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3045
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-QCA6-071122/3046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3047
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3048
Product: qca6564au					
Affected Version(s): -					
Buffer Copy without	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing	https://www.qualcomm.com/compa	H-QUA-QCA6-071122/3049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	ny/product-security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3050
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/3051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3052
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25660		
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3054
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3055
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3056
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-071122/3057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3058
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-QCA6-071122/3059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3060
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3061
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/3062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	r-2022-bulletin	
Product: qca6574					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3063
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3065
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3067
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3068
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3070
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3071
Time-of-check	19-Oct-2022	7	Memory corruption in display due to time-of-	https://www.qualcomm	H-QUA-QCA6-071122/3072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	.com/company/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3073
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3075
Product: qca6574a					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3076
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/3077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3078
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3080
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3081
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/3082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3083
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3085
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3086
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33214		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3088
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3089
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: qca6574au					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3091
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3093
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3095
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3096
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3097
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-071122/3098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3099
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3101
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3102
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3104
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3105
Product: qca6584					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3106
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3108
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3110
Product: qca6584au					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3112
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3114
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3115
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3117
Product: qca6595					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/3118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	r-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3119
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3121
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3123
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3124
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3126
Product: qca6595au					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3127
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper	https://www.qualcomm	H-QUA-QCA6-071122/3128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	.com/company/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3129
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing	https://www.qualcomm.com/company/product-	H-QUA-QCA6-071122/3130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	security/bulletins/october-2022-bulletin	
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3131
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3133
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3134
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3136
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3137
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/3138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3139
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3140
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-071122/3141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	etins/october-2022-bulletin	
Product: qca6694					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3142
Product: qca6696					
Affected Version(s): -					
Buffer Copy without	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing	https://www.qualcomm.com/compa	H-QUA-QCA6-071122/3143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	ny/product-security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3144
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-071122/3145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3146
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25660		
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3148
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3149
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3150
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-071122/3151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3152
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-QCA6-071122/3153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	security/bulletins/october-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3154
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3155
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA6-071122/3157
Product: qca7500					
Affected Version(s): -					
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA7-071122/3158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Product: qca8072					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3159
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3161
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: qca8075					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3163
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3165
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3167
Product: qca8081					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3169
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3171
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3172
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3174
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3176
Product: qca8082					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3178
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Product: qca8084					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3180
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3182
Product: qca8085					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3184
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qca8337					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3186
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3188
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3189
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA8-071122/3190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3191
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA8-071122/3192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	etins/octobe r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://ww w.qualcomm .com/compa ny/product-security/bull etins/octobe r-2022-bulletin	H-QUA-QCA8-071122/3193
Exposure of Sensitive Informati on to an Unauthori zed Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://ww w.qualcomm .com/compa ny/product-security/bull etins/octobe r-2022-bulletin	H-QUA-QCA8-071122/3194
Integer Overflow or Wraparou nd	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto,	https://ww w.qualcomm .com/compa ny/product-security/bull etins/octobe	H-QUA-QCA8-071122/3195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	r-2022-bulletin	
Product: qca8386					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3196
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA8-071122/3197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA8-071122/3198
Product: qca9367					
Affected Version(s): -					
Buffer Copy without	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing	https://www.qualcomm.com/compa	H-QUA-QCA9-071122/3199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	ny/product-security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3200
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA9-071122/3201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3202
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qca9369					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3204
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA9-071122/3205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	etins/october-2022-bulletin	
Product: qca9377					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3206
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA9-071122/3207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3208
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3210
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA9-071122/3211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3212
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3213
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA9-071122/3214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3215
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22078		
Product: qca9379					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3217
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3219
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3221
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Product: qca9880					
Affected Version(s): -					
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3223
Product: qca9886					
Affected Version(s): -					
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3224
Product: qca9888					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3225
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3227
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3229
Product: qca9889					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3231
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3233
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Product: qca9898					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3235
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3237
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: qca9980					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3239
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3241
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: qca9984					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3243
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3245
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: qca9985					
Affected Version(s): -					
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3247
Product: qca9990					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3249
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3251
Product: qca9992					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3253
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3255
Product: qca9994					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3257
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCA9-071122/3259
Product: qcc5100					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCC5-071122/3260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCC5-071122/3261
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCC5-071122/3262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCC5-071122/3263
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCC5-071122/3264
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCC5-071122/3265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCC5-071122/3266
Time-of-check Time-of-use (TOCTOU	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCC5-071122/3267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
) Race Condition			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	etins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCC5-071122/3268
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCC5-071122/3269
Product: qcm2290					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM2-071122/3270
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM2-071122/3271
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT	https://www.qualcomm.com/company/product-	H-QUA-QCM2-071122/3272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM2-071122/3273
Time-of-check Time-of-	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of	https://www.qualcomm.com/compa	H-QUA-QCM2-071122/3274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	ny/product-security/bulletins/october-2022-bulletin	
Product: qcm4290					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM4-071122/3275
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM4-071122/3276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM4-071122/3277
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM4-071122/3278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM4-071122/3279
Product: qcm6125					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM6-071122/3280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM6-071122/3281
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM6-071122/3282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM6-071122/3283
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM6-071122/3284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM6-071122/3285
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM6-071122/3286
Product: qcm6490					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM6-071122/3287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM6-071122/3288
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM6-071122/3289
Release of Invalid	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in	https://www.qualcomm.com/compa	H-QUA-QCM6-071122/3290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM6-071122/3291
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM6-071122/3292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCM6-071122/3293
Product: qcn5021					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3295
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3297
Product: qcn5022					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3299
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3301
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: qcn5024					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3303
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3305
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3307
Product: qcn5052					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3309
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3311
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: qcn5054					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3313
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3315
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: qcn5122					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3317
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3319
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCN5-071122/3320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3321
Product: qcn5124					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3323
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCN5-071122/3324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3325
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCN5-071122/3326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Product: qcn5152					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3327
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCN5-071122/3328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3329
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCN5-071122/3330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	etins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3331
Product: qcn5154					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCN5-071122/3332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3333
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT	https://www.qualcomm.com/company/product-	H-QUA-QCN5-071122/3334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3335
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to	https://www.qualcomm.com/compa	H-QUA-QCN5-071122/3336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	ny/product-security/bulletins/october-2022-bulletin	
Product: qcn5164					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3337
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing	https://www.qualcomm.com/company/product-	H-QUA-QCN5-071122/3338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3340
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN5-071122/3341
Product: qcn6023					
Affected Version(s): -					
Integer Overflow	19-Oct-2022	9.8	Memory corruption in WLAN due to integer	https://www.qualcomm	H-QUA-QCN6-071122/3342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25719		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3344
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3346
Product: qcn6024					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3348
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3350
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3352
Product: qcn6100					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3354
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qcn6102					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3356
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3358
Product: qcn6112					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3360
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCN6-071122/3361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Product: qcn6122					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3363
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3365
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3366
Product: qcn6132					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3367
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3369
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN6-071122/3371
Product: qcn7605					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN7-071122/3372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN7-071122/3373
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN7-071122/3374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN7-071122/3375
Product: qcn7606					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN7-071122/3376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25687		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN7-071122/3377
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN7-071122/3378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN7-071122/3379
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN7-071122/3380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN7-071122/3381
Product: qcn9000					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3383
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3385
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcn9001					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3387
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3389
Product: qcn9002					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3391
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qcn9003					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3393
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCN9-071122/3394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3395
Product: qcn9011					
Affected Version(s): -					
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer	https://www.qualcomm.com/compa	H-QUA-QCN9-071122/3396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	ny/product-security/bulletins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3397
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3399
Product: qcn9012					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3401
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3403
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Product: qcn9022					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3405
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3407
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3409
Product: qcn9024					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3411
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3413
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3415
Product: qcn9070					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3417
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3419
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: qcn9072					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3421
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3423
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3425
Product: qcn9074					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3427
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3429
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: qcn9100					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3431
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3433
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCN9-071122/3434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3435
Product: qcn9274					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCN9-071122/3437
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCN9-071122/3438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Product: qcs2290					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS2-071122/3439
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS2-071122/3440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS2-071122/3441
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCS2-071122/3442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS2-071122/3443
Product: qcs405					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3445
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3447
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3449
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qcs410					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3451
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3453
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3455
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3457
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3458
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: qcs4290					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3460
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3462
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS4-071122/3464
Product: qcs603					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3466
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3467
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3469
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3470
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCS6-071122/3471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	r-2022-bulletin	
Product: qcs605					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3472
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3474
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3475
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCS6-071122/3476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3477
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3479
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3480
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: qcs610					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3482
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3484
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3485
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens	https://www.qualcomm.com/compa	H-QUA-QCS6-071122/3486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3488
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3489
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25664		
Product: qcs6125					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3491
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3492
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer	https://www.qualcomm.com/compa	H-QUA-QCS6-071122/3493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3495
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3496
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCS6-071122/3497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	r-2022-bulletin	
Product: qcs6490					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3498
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3500
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3501
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3503
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS6-071122/3504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcs8155					
Affected Version(s): -					
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS8-071122/3505
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS8-071122/3506
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCS8-071122/3507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: qcx315					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCX3-071122/3508
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCX3-071122/3509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCX3-071122/3510
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QCX3-071122/3511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qet4101					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QET4-071122/3512
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QET4-071122/3513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QET4-071122/3514
Product: qrb5165					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QRB5-071122/3515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QRB5-071122/3516
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QRB5-071122/3517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QRB5-071122/3518
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QRB5-071122/3519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qrb5165m					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QRB5-071122/3520
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QRB5-071122/3521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QRB5-071122/3522
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QRB5-071122/3523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QRB5-071122/3524
Product: qrb5165n					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QRB5-071122/3525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QRB5-071122/3526
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QRB5-071122/3527
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QRB5-071122/3528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QRB5-071122/3529
Product: qsm8250					
Affected Version(s): -					
Integer Overflow	19-Oct-2022	9.8	Memory corruption in WLAN due to integer	https://www.qualcomm	H-QUA-QSM8-071122/3530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QSM8-071122/3531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QSM8-071122/3532
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QSM8-071122/3533
Exposure of Sensitive Information to an	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QSM8-071122/3534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	etins/october-2022-bulletin	
Product: qsm8350					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QSM8-071122/3535
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QSM8-071122/3536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QSM8-071122/3537
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QSM8-071122/3538
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QSM8-071122/3539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QSM8-071122/3540
Product: qsw8573					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QSW8-071122/3541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QSW8-071122/3542
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QSW8-071122/3543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: qualcomm215					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QUAL-071122/3544
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QUAL-071122/3545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QUAL-071122/3546
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QUAL-071122/3547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QUAL-071122/3548
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-QUAL-071122/3549
Product: sa4150p					
Affected Version(s): -					
Buffer Copy without Checking	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-SA41-071122/3550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3551
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3553
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3555
Product: sa4155p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25687		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3557
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3559
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3561
Product: sa415m					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3563
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3565
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA41-071122/3567
Product: sa515m					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA51-071122/3568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA51-071122/3569
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA51-071122/3570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA51-071122/3571
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA51-071122/3572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA51-071122/3573
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA51-071122/3574
Product: sa6145p					
Affected Version(s): -					
Buffer Copy	19-Oct-2022	9.8	memory corruption in video due to buffer	https://www.qualcomm	H-QUA-SA61-071122/3575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	.com/company/product-security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3576
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SA61-071122/3577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3578
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SA61-071122/3579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3580
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3581
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3583
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3585
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3586
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3588
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3589
Product: sa6150p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3591
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3593
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3594
Release of Invalid	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in	https://www.qualcomm.com/compa	H-QUA-SA61-071122/3595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3596
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3598
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3600
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3601
Product: sa6155					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3603
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3605
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3606
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3608
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3610
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3611
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3613
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3614
Product: sa6155p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3616
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3618
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3619
Release of Invalid	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in	https://www.qualcomm.com/compa	H-QUA-SA61-071122/3620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3621
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3622
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3624
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25665		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3626
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3627
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA61-071122/3629
Product: sa8145p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3630
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper	https://www.qualcomm	H-QUA-SA81-071122/3631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	.com/company/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3632
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing	https://www.qualcomm.com/company/product-	H-QUA-SA81-071122/3633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	security/bulletins/october-2022-bulletin	
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3634
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25662		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3636
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3638
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3639
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3641
Product: sa8150p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3643
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3645
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3646
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25661		
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3648
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3649
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3651
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3652
Time-of-check Time-of-use (TOCTOU	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA81-071122/3653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
) Race Condition			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	etins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3654
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3655
Integer Overflow or	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is	https://www.qualcomm.com/compa	H-QUA-SA81-071122/3656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	ny/product-security/bulletins/october-2022-bulletin	
Product: sa8155					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3657
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3659
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3661
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3662
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33210		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3664
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3666
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3667
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3669
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3670
Product: sa8155p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SA81-071122/3671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	r-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3672
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3674
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3676
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3677
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3678
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SA81-071122/3679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3680
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SA81-071122/3681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	r-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3682
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3683
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3685
Product: sa8195p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3687
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3689
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3690
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3692
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3694
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3695
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA81-071122/3697
Product: sa8295p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA82-071122/3698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25687		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA82-071122/3699
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA82-071122/3700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA82-071122/3701
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA82-071122/3702
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA82-071122/3703
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA82-071122/3704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA82-071122/3705
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA82-071122/3706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA82-071122/3707
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA82-071122/3708
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA82-071122/3709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA82-071122/3710
Product: sa8540p					
Affected Version(s): -					
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA85-071122/3711
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA85-071122/3712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA85-071122/3713
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA85-071122/3714
Product: sa9000p					
Affected Version(s): -					
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA90-071122/3715
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA90-071122/3716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25661		
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA90-071122/3717
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SA90-071122/3718
Product: sc8180x\+sdx55					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SC81-071122/3719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SC81-071122/3720
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SC81-071122/3721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: sd205					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD20-071122/3722
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD20-071122/3723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD20-071122/3724
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD20-071122/3725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD20-071122/3726
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD20-071122/3727
Product: sd210					
Affected Version(s): -					
Buffer Copy without Checking	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-SD21-071122/3728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD21-071122/3729
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD21-071122/3730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD21-071122/3731
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD21-071122/3732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD21-071122/3733
Product: sd429					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD42-071122/3734
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper	https://www.qualcomm	H-QUA-SD42-071122/3735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	.com/company/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD42-071122/3736
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing	https://www.qualcomm.com/company/product-	H-QUA-SD42-071122/3737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	security/bulletins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD42-071122/3738
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD42-071122/3739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD42-071122/3740
Product: sd439					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD43-071122/3741
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper	https://www.qualcomm	H-QUA-SD43-071122/3742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	.com/company/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD43-071122/3743
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing	https://www.qualcomm.com/company/product-	H-QUA-SD43-071122/3744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	security/bulletins/october-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD43-071122/3745
Product: sd450					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD45-071122/3746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD45-071122/3747
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD45-071122/3748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD45-071122/3749
Product: sd460					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD46-071122/3750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD46-071122/3751
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD46-071122/3752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD46-071122/3753
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD46-071122/3754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD46-071122/3755
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD46-071122/3756
Product: sd480					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD48-071122/3757
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD48-071122/3758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD48-071122/3759
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD48-071122/3760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD48-071122/3761
Product: sd632					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD63-071122/3762
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD63-071122/3763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD63-071122/3764
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD63-071122/3765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: sd660					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3766
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3768
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3770
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3772
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3773
Product: sd662					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3774
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3775
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD66-071122/3776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3777
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD66-071122/3778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3779
Product: sd665					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3781
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD66-071122/3783
Product: sd670					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3785
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3787
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3788
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3790
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3791
Product: sd675					
Affected Version(s): -					
Buffer Copy without	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing	https://www.qualcomm.com/compa	H-QUA-SD67-071122/3792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	ny/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3793
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3795
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3796
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3798
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD67-071122/3799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25665	r-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3800
Product: sd678					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3801
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3803
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25660		
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3805
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3806
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD67-071122/3807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3808
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD67-071122/3809
Product: sd680					
Affected Version(s): -					
Buffer Copy	19-Oct-2022	9.8	memory corruption in video due to buffer	https://www.qualcomm	H-QUA-SD68-071122/3810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	.com/company/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD68-071122/3811
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD68-071122/3812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD68-071122/3813
Time-of-check Time-of-use (TOCTOU	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD68-071122/3814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
) Race Condition			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	etins/october-2022-bulletin	
Product: sd690_5g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD69-071122/3815
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD69-071122/3816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD69-071122/3817
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD69-071122/3818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD69-071122/3819
Product: sd695					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD69-071122/3820
Integer Overflow	19-Oct-2022	9.8	Memory corruption in WLAN due to integer	https://www.qualcomm	H-QUA-SD69-071122/3821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD69-071122/3822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD69-071122/3823
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD69-071122/3824
Product: sd710					
Affected Version(s): -					
Buffer Copy without Checking Size of	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD71-071122/3825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	etins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD71-071122/3826
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD71-071122/3827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD71-071122/3828
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD71-071122/3829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD71-071122/3830
Product: sd712					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD71-071122/3831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD71-071122/3832
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD71-071122/3833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: sd720g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD72-071122/3834
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD72-071122/3835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD72-071122/3836
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD72-071122/3837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD72-071122/3838
Product: sd730					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD73-071122/3839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD73-071122/3840
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD73-071122/3841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD73-071122/3842
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD73-071122/3843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD73-071122/3844
Product: sd750g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD75-071122/3845
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD75-071122/3846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD75-071122/3847
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD75-071122/3848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD75-071122/3849
Product: sd765					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3851
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3852
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD76-071122/3853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3854
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3856
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3857
Product: sd765g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3859
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3860
Release of Invalid	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in	https://www.qualcomm.com/compa	H-QUA-SD76-071122/3861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3862
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3864
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3865
Product: sd768g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3867
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3869
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3870
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3872
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD76-071122/3873
Product: sd778g					
Affected Version(s): -					
Buffer Copy without Checking Size of	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD77-071122/3874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD77-071122/3875
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD77-071122/3876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25660		
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD77-071122/3877
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD77-071122/3878
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD77-071122/3879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD77-071122/3880
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD77-071122/3881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD77-071122/3882
Product: sd780g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD78-071122/3883
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD78-071122/3884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD78-071122/3885
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD78-071122/3886
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD78-071122/3887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD78-071122/3888
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD78-071122/3889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD78-071122/3890
Product: sd7c					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD7C-071122/3891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD7C-071122/3892
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD7C-071122/3893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD7C-071122/3894
Product: sd820					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD82-071122/3895
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD82-071122/3896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD82-071122/3897
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD82-071122/3898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD82-071122/3899
Exposure of Sensitive Information to an	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD82-071122/3900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	r-2022-bulletin	
Product: sd821					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD82-071122/3901
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD82-071122/3902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD82-071122/3903
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD82-071122/3904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD82-071122/3905
Product: sd835					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD83-071122/3906
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value	https://www.qualcomm.com/compa	H-QUA-SD83-071122/3907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	ny/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD83-071122/3908
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD83-071122/3909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	etins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD83-071122/3910
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD83-071122/3911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD83-071122/3912
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD83-071122/3913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD83-071122/3914
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD83-071122/3915
Product: sd845					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD84-071122/3916
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD84-071122/3917
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD84-071122/3918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD84-071122/3919
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD84-071122/3920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD84-071122/3921
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD84-071122/3922
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD84-071122/3923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD84-071122/3924
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD84-071122/3925
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in	https://www.qualcomm	H-QUA-SD84-071122/3926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	.com/company/product-security/bulletins/october-2022-bulletin	
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD84-071122/3927
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD84-071122/3928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: sd850					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3929
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3930
Release of Invalid	19-Oct-2022	7.8	Memory corruption due to untrusted pointer	https://www.qualcomm	H-QUA-SD85-071122/3931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3932
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3934
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3935
Product: sd855					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3937
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3939
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3940
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3942
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3943
Time-of-check Time-of-	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of	https://www.qualcomm.com/compa	H-QUA-SD85-071122/3944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	ny/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3945
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD85-071122/3947
Product: sd865_5g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD86-071122/3948
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD86-071122/3949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD86-071122/3950
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD86-071122/3951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD86-071122/3952
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD86-071122/3953
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD86-071122/3954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD86-071122/3955
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD86-071122/3956
Time-of-check	19-Oct-2022	7	Memory corruption in display due to time-of-	https://www.qualcomm	H-QUA-SD86-071122/3957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	.com/company/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD86-071122/3958
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD86-071122/3959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD86-071122/3960
Product: sd870					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD87-071122/3961
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD87-071122/3962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD87-071122/3963
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD87-071122/3964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD87-071122/3965
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD87-071122/3966
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD87-071122/3967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD87-071122/3968
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD87-071122/3969
Time-of-check	19-Oct-2022	7	Memory corruption in display due to time-of-	https://www.qualcomm	H-QUA-SD87-071122/3970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	.com/company/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD87-071122/3971
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD87-071122/3972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD87-071122/3973
Product: sd888					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD88-071122/3974
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD88-071122/3975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	r-2022-bulletin	
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD88-071122/3976
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD88-071122/3977
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD88-071122/3978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD88-071122/3979
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD88-071122/3980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD88-071122/3981
Product: sd888_5g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD88-071122/3982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD88-071122/3983
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD88-071122/3984
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD88-071122/3985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25661		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD88-071122/3986
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD88-071122/3987
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in	https://www.qualcomm.com/company/product-	H-QUA-SD88-071122/3988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD88-071122/3989
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD88-071122/3990
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in	https://www.qualcomm	H-QUA-SD88-071122/3991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	.com/company/product-security/bulletins/october-2022-bulletin	
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD88-071122/3992
Product: sda429w					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDA4-071122/3993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDA4-071122/3994
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDA4-071122/3995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDA4-071122/3996
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDA4-071122/3997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDA4-071122/3998
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDA4-071122/3999
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDA4-071122/4000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25664		
Product: sdm429w					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDM4-071122/4001
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDM4-071122/4002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDM4-071122/4003
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDM4-071122/4004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDM4-071122/4005
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDM4-071122/4006
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDM4-071122/4007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: sdm630					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDM6-071122/4008
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDM6-071122/4009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDM6-071122/4010
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDM6-071122/4011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: sdw2500					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDW2-071122/4012
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDW2-071122/4013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDW2-071122/4014
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDW2-071122/4015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: sdx12					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX1-071122/4016
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX1-071122/4017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX1-071122/4018
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX1-071122/4019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: sdx20					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4020
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4022
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4024
Product: sdx20m					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4026
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4028
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: sdx24					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4030
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4032
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4033
Release of Invalid	19-Oct-2022	7.8	Memory corruption due to untrusted pointer	https://www.qualcomm	H-QUA-SDX2-071122/4034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4035
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX2-071122/4036
Integer Overflow	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a	https://www.qualcomm	H-QUA-SDX2-071122/4037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	.com/company/product-security/bulletins/october-2022-bulletin	
Product: sdx50m					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4038
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4040
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25660		
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4042
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4043
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SDX5-071122/4044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4045
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4046
Exposure of Sensitive Information to an	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDX5-071122/4047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	etins/october-2022-bulletin	
Product: sdx55					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4048
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4050
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4052
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4053
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4055
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4056
Time-of-check Time-of-	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of	https://www.qualcomm.com/compa	H-QUA-SDX5-071122/4057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	ny/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4058
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4060
Product: sdx55m					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4061
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SDX5-071122/4062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4063
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SDX5-071122/4064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4065
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4066
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4068
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4069
Time-of-check	19-Oct-2022	7	Memory corruption in display due to time-of-	https://www.qualcomm	H-QUA-SDX5-071122/4070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	.com/company/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4071
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4073
Product: sdx57m					
Affected Version(s): -					
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4074
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX5-071122/4076
Product: sdx65					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX6-071122/4077
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX6-071122/4078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX6-071122/4079
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX6-071122/4080
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX6-071122/4081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX6-071122/4082
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDX6-071122/4083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25665		
Product: sdxr1					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4084
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4085
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer	https://www.qualcomm.com/compa	H-QUA-SDXR-071122/4086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	ny/product-security/bulletins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4087
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4089
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SDXR-071122/4090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	r-2022-bulletin	
Product: sdxr2_5g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4091
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4093
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4094
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SDXR-071122/4095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4096
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4098
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4099
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4101
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SDXR-071122/4102
Product: sd_455					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value	https://www.qualcomm.com/compa	H-QUA-SD_4-071122/4103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	ny/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_4-071122/4104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_4-071122/4105
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_4-071122/4106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Product: sd_636					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_6-071122/4107
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_6-071122/4108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_6-071122/4109
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_6-071122/4110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_6-071122/4111
Product: sd_675					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_6-071122/4112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_6-071122/4113
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_6-071122/4114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_6-071122/4115
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_6-071122/4116
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_6-071122/4117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_6-071122/4118
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_6-071122/4119
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_6-071122/4120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**		
Product: sd_8cx					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4121
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4122
Release of Invalid	19-Oct-2022	7.8	Memory corruption due to untrusted pointer	https://www.qualcomm	H-QUA-SD_8-071122/4123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4124
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4126
Product: sd_8cx_gen2					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4128
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4129
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4131
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4132
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD_8-071122/4133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	r-2022-bulletin	
Product: sd_8cx_gen3					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4134
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4136
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4137
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4139
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4140
Product: sd_8_gen1_5g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD_8-071122/4141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4142
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4144
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4145
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4146
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback	https://www.qualcomm.com/company/product-	H-QUA-SD_8-071122/4147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	security/bulletins/october-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4148
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4149
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4151
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4152
Time-of-check Time-of-	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of	https://www.qualcomm.com/compa	H-QUA-SD_8-071122/4153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	ny/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4154
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SD_8-071122/4155
Product: sg8275					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SG82-071122/4156
Product: sg8275p					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SG82-071122/4157
Product: sm4125					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM41-071122/4158
Improper Validation	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access	https://www.qualcomm.com/compa	H-QUA-SM41-071122/4159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	ny/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM41-071122/4160
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT	https://www.qualcomm.com/company/product-	H-QUA-SM41-071122/4161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM41-071122/4162
Time-of-check Time-of-	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of	https://www.qualcomm.com/compa	H-QUA-SM41-071122/4163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	ny/product-security/bulletins/october-2022-bulletin	
Product: sm4375					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM43-071122/4164
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM43-071122/4165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM43-071122/4166
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM43-071122/4167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM43-071122/4168
Product: sm6250					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM62-071122/4169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM62-071122/4170
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM62-071122/4171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM62-071122/4172
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM62-071122/4173
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM62-071122/4174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	etins/october-2022-bulletin	
Product: sm6250p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM62-071122/4175
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM62-071122/4176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM62-071122/4177
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM62-071122/4178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: sm7250p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM72-071122/4179
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM72-071122/4180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM72-071122/4181
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM72-071122/4182
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM72-071122/4183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM72-071122/4184
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM72-071122/4185
Time-of-check Time-of-use	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size	https://www.qualcomm.com/company/product-	H-QUA-SM72-071122/4186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	security/bulletins/october-2022-bulletin	
Product: sm7315					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM73-071122/4187
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM73-071122/4188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM73-071122/4189
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM73-071122/4190
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM73-071122/4191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25662		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM73-071122/4192
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM73-071122/4193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM73-071122/4194
Product: sm7325p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM73-071122/4195
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SM73-071122/4196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	r-2022-bulletin	
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM73-071122/4197
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM73-071122/4198
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SM73-071122/4199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM73-071122/4200
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM73-071122/4201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM73-071122/4202
Product: sm8550					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SM85-071122/4203
Product: sw5100					
Affected Version(s): -					
Buffer Copy without Checking Size of	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-SW51-071122/4204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	etins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4205
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4207
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4209
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4211
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4212
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4214
Product: sw5100p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25687		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4216
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4218
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4219
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens	https://www.qualcomm.com/compa	H-QUA-SW51-071122/4220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4222
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4223
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25664		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SW51-071122/4225
Product: sxr2150p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SXR2-071122/4226
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in	https://www.qualcomm.com/company/product-security/bull	H-QUA-SXR2-071122/4227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SXR2-071122/4228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-SXR2-071122/4229
Product: wcd9306					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4231
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: wcd9326					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4233
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4235
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4237
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4238
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCD9-071122/4239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4240
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4242
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4243
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33214		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4245
Product: wcd9330					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4246
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCD9-071122/4247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4248
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4250
Product: wcd9335					
Affected Version(s): -					
Buffer Copy without Checking	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-WCD9-071122/4251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4252
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4254
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4256
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4258
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4260
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4261
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: wcd9340					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4263
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4265
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4267
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4268
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCD9-071122/4269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	etins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4270
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4272
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4273
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4275
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4276
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: wcd9341					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4278
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4280
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4282
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4283
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4285
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4287
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4288
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4290
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4291
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22078		
Product: wcd9360					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4293
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4295
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4297
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: wcd9370					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4299
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4301
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4303
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4304
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4305
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCD9-071122/4306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4307
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-WCD9-071122/4308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	security/bulletins/october-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4309
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4310
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: wcd9371					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4312
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4314
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4316
Product: wcd9375					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25687		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4318
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4320
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4321
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCD9-071122/4322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4323
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4325
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4326
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33214		
Product: wcd9380					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4328
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4329
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer	https://www.qualcomm.com/compa	H-QUA-WCD9-071122/4330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	ny/product-security/bulletins/october-2022-bulletin	
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4331
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4332
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCD9-071122/4333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4334
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4335
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4336
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4338
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4340
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4341
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4343
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4344
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: wcd9385					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4346
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4348
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4349
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4351
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4352
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4354
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4355
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCD9-071122/4356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4357
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4358
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4360
Product: wcd9390					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCD9-071122/4361
Product: wcd9395					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCD9-071122/4362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	etins/october-2022-bulletin	
Product: wcn3610					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4363
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4365
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4367
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4368
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while	https://www.qualcomm.com/compa	H-QUA-WCN3-071122/4369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	ny/product-security/bulletins/october-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4370
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4372
Product: wcn3615					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4373
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value	https://www.qualcomm.com/compa	H-QUA-WCN3-071122/4374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	ny/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4375
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-071122/4376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4378
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4379
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN3-071122/4380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	r-2022-bulletin	
Product: wcn3620					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4381
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4383
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4385
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4386
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: wcn3660					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4388
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4390
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: wcn3660b					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4392
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4394
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4396
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4397
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while	https://www.qualcomm.com/compa	H-QUA-WCN3-071122/4398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	ny/product-security/bulletins/october-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4399
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4401
Product: wcn3680					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4402
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value	https://www.qualcomm.com/compa	H-QUA-WCN3-071122/4403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	ny/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4404
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-071122/4405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	etins/october-2022-bulletin	
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4406
Product: wcn3680b					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN3-071122/4407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	r-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4408
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4410
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4412
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4414
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4415
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: wcn3910					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4417
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4419
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4421
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4422
Product: wcn3950					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4423
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4424
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-071122/4425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4426
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN3-071122/4427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4428
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4429
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4431
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4432
Time-of-check	19-Oct-2022	7	Memory corruption in display due to time-of-	https://www.qualcomm	H-QUA-WCN3-071122/4433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	.com/company/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4434
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcn3980					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4436
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4437
Improper Validation	19-Oct-2022	9.8	Memory corruption in WLAN due to out of	https://www.qualcomm	H-QUA-WCN3-071122/4438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	.com/company/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4440
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4441
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25661		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4443
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4444
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in	https://www.qualcomm.com/company/product-	H-QUA-WCN3-071122/4445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4446
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4447
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in	https://www.qualcomm	H-QUA-WCN3-071122/4448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	.com/company/product-security/bulletins/october-2022-bulletin	
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4449
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: wcn3988					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4451
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4453
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4455
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4456
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in	https://www.qualcomm.com/company/product-	H-QUA-WCN3-071122/4457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	security/bulletins/october-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4458
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4460
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4461
Product: wcn3990					
Affected Version(s): -					
Buffer Copy without	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing	https://www.qualcomm.com/compa	H-QUA-WCN3-071122/4462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	ny/product-security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4463
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN3-071122/4464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4465
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25660		
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4467
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4468
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4470
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4471
Time-of-check Time-of-use	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size	https://www.qualcomm.com/company/product-	H-QUA-WCN3-071122/4472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4473
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4474
Exposure of Sensitive Information to an	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-071122/4475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4476
Product: wcn3991					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4478
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4479
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-071122/4480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4481
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4483
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4484
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcn3998					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4486
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4487
Improper Validation	19-Oct-2022	9.8	Memory corruption in WLAN due to out of	https://www.qualcomm	H-QUA-WCN3-071122/4488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	.com/company/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4490
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4491
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25661		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4493
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4495
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4496
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4498
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4499
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: wcn3999					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4501
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4503
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4505
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN3-071122/4507
Product: wcn6740					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25687		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4509
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4511
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4512
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4513
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN6-071122/4514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4515
Time-of-check Time-of-use	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size	https://www.qualcomm.com/company/product-	H-QUA-WCN6-071122/4516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	security/bulletins/october-2022-bulletin	
Product: wcn6750					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4517
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4519
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4520
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25662		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4522
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4524
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4525
Product: wcn6850					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4527
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4529
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4530
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4532
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4534
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4535
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4537
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4538
Product: wcn6851					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4540
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4542
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4543
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25662		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4545
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4547
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4548
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4550
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4551
Product: wcn6855					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN6-071122/4552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4553
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4555
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4556
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4557
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN6-071122/4558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	r-2022-bulletin	
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4559
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4560
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4561
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN6-071122/4562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4563
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN6-071122/4564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	etins/octobe r-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://ww w.qualcomm .com/compa ny/product-security/bull etins/octobe r-2022-bulletin	H-QUA-WCN6-071122/4565
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://ww w.qualcomm .com/compa ny/product-security/bull etins/octobe r-2022-bulletin	H-QUA-WCN6-071122/4566
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcomm .com/compa ny/product-security/bull etins/octobe r-2022-bulletin	H-QUA-WCN6-071122/4567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4568
Product: wcn6856					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4569
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming	https://www.qualcomm.com/company/product-	H-QUA-WCN6-071122/4570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4571
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN6-071122/4572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	etins/octobe r-2022-bulletin	
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://ww w.qualcomm .com/compa ny/product-security/bull etins/octobe r-2022-bulletin	H-QUA-WCN6-071122/4573
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://ww w.qualcomm .com/compa ny/product-security/bull etins/octobe r-2022-bulletin	H-QUA-WCN6-071122/4574
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://ww w.qualcomm .com/compa ny/product-security/bull etins/octobe r-2022-bulletin	H-QUA-WCN6-071122/4575
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	https://ww w.qualcomm .com/compa ny/product-security/bull etins/octobe r-2022-bulletin	H-QUA-WCN6-071122/4576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4577
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4578
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4580
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4581
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN6-071122/4582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4583
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4584
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN6-071122/4585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: wcn7850					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4586
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4588
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4589
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4591
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4592
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4593
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4594
Release of Invalid	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in	https://www.qualcomm.com/compa	H-QUA-WCN7-071122/4595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4596
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4598
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4599
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4601
Product: wcn7851					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4603
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4605
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4606
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4607
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4608
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN7-071122/4609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	etins/october-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4610
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4611
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4613
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4614
Time-of-check Time-of-	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of	https://www.qualcomm.com/compa	H-QUA-WCN7-071122/4615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	ny/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4616
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WCN7-071122/4617
Product: wsa8810					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4618
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4619
Improper Validation	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access	https://www.qualcomm.com/compa	H-QUA-WSA8-071122/4620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	ny/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4621
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing	https://www.qualcomm.com/company/product-	H-QUA-WSA8-071122/4622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	security/bulletins/october-2022-bulletin	
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4623
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4624
Release of Invalid	19-Oct-2022	7.5	Information disclosure due to untrusted pointer	https://www.qualcomm	H-QUA-WSA8-071122/4625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4626
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4628
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4629
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WSA8-071122/4630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4631
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4632
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WSA8-071122/4633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	r-2022-bulletin	
Product: wsa8815					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4634
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4636
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4638
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4640
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4641
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4643
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4644
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WSA8-071122/4645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4646
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4647
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4649
Product: wsa8830					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25687		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4651
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4653
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4654
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25660		
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4656
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4657
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4658
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4660
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4662
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4663
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4665
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4666
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: wsa8835					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4668
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4670
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4672
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4673
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4674
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4675
Buffer Copy without	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without	https://www.qualcomm.com/compa	H-QUA-WSA8-071122/4676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	ny/product-security/bulletins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4677
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4679
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4680
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4682
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4683
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4685
Product: wsa8840					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4686
Product: wsa8845					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WSA8-071122/4687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25750	r-2022-bulletin	
Product: wsa8845h					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	H-QUA-WSA8-071122/4688
Vendor: robustel					
Product: r1510					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	9.8	An OS command injection vulnerability exists in the sysupgrade command injection functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-32765**	N/A	H-ROB-R151-071122/4689
Improper Neutralization of Special Elements used in an OS Command ('OS	25-Oct-2022	9.8	An OS command injection vulnerability exists in the js_package install functionality of Robustel R1510 3.1.16. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of	N/A	H-ROB-R151-071122/4690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			requests to trigger this vulnerability. **CVE ID : CVE-2022-33150**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Oct-2022	9.1	A directory traversal vulnerability exists in the web_server /ajax/remove/ functionality of Robustel R1510 3.1.16. A specially-crafted network request can lead to arbitrary file deletion. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-33897**	N/A	H-ROB-R151-071122/4691
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_authorized_keys/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35261**	N/A	H-ROB-R151-071122/4692
Improper Neutralization of Special Elements used in a	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted	N/A	H-ROB-R151-071122/4693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_xml_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35262**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35263**	N/A	H-ROB-R151-071122/4694
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_aaa_cert	N/A	H-ROB-R151-071122/4695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35264**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_nodejs_app/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35265**	N/A	H-ROB-R151-071122/4696
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_firmware/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35266**	N/A	H-ROB-R151-071122/4697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_https_cert_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35267**	N/A	H-ROB-R151-071122/4698
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_sdk_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35268**	N/A	H-ROB-R151-071122/4699
Improper Neutralization of Special Elements used in a Command	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead	N/A	H-ROB-R151-071122/4700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_e2c_json_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35269**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_wireguard_cert_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35270**	N/A	H-ROB-R151-071122/4701
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_cert_file/` API is affected by	N/A	H-ROB-R151-071122/4702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection vulnerability. **CVE ID : CVE-2022-35271**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	7.2	An OS command injection vulnerability exists in the web_server /action/import_authorized_keys/ functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-34850**	N/A	H-ROB-R151-071122/4703
Insufficient Verification of Data Authenticity	25-Oct-2022	2.7	A firmware update vulnerability exists in the sysupgrade functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network packet can lead to arbitrary firmware update. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-34845**	N/A	H-ROB-R151-071122/4704
Vendor: Synology					
Product: ds3622xs\+					
Affected Version(s): -					
Improper Restriction of Operations within the	20-Oct-2022	9.8	A vulnerability regarding improper restriction of operations within the bounds of a memory buffer is found in the packet decryption	https://www.synology.com/security/advisory/Synology_SA_22_17	H-SYN-DS36-071122/4705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-27624**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-2022	9.8	A vulnerability regarding improper restriction of operations within the bounds of a memory buffer is found in the message processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-27625**	https://www.synology.com/security/advisory/Synology_SA_22_17	H-SYN-DS36-071122/4706
Concurrent Execution using Shared	20-Oct-2022	8.1	A vulnerability regarding concurrent execution using shared resource with improper synchronization ('Race	https://www.synology.com/security/advisory/S	H-SYN-DS36-071122/4707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			Condition') is found in the session processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-27626**	ynology_SA_22_17	
Out-of-bounds Read	20-Oct-2022	7.5	A vulnerability regarding out-of-bounds read is found in the session processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to obtain sensitive information via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-3576**	https://www.synology.com/security/advisory/Synology_SA_22_17	H-SYN-DS36-071122/4708
Product: fs3410					
Affected Version(s): -					
Improper Restriction of	20-Oct-2022	9.8	A vulnerability regarding improper restriction of operations within the	https://www.synology.com/security	H-SYN-FS34-071122/4709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			bounds of a memory buffer is found in the packet decryption functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-27624**	/advisory/Synology_SA_22_17	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-2022	9.8	A vulnerability regarding improper restriction of operations within the bounds of a memory buffer is found in the message processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-27625**	https://www.synology.com/security/advisory/Synology_SA_22_17	H-SYN-FS34-071122/4710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	20-Oct-2022	8.1	A vulnerability regarding concurrent execution using shared resource with improper synchronization ('Race Condition') is found in the session processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-27626**	https://www.synology.com/security/advisory/Synology_SA_22_17	H-SYN-FS34-071122/4711
Out-of-bounds Read	20-Oct-2022	7.5	A vulnerability regarding out-of-bounds read is found in the session processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to obtain sensitive information via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-3576**	https://www.synology.com/security/advisory/Synology_SA_22_17	H-SYN-FS34-071122/4712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: hd6500					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-2022	9.8	A vulnerability regarding improper restriction of operations within the bounds of a memory buffer is found in the packet decryption functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-27624**	https://www.synology.com/security/advisory/Synology_SA_22_17	H-SYN-HD65-071122/4713
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-2022	9.8	A vulnerability regarding improper restriction of operations within the bounds of a memory buffer is found in the message processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected:	https://www.synology.com/security/advisory/Synology_SA_22_17	H-SYN-HD65-071122/4714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-27625**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	20-Oct-2022	8.1	A vulnerability regarding concurrent execution using shared resource with improper synchronization ('Race Condition') is found in the session processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-27626**	https://www.synology.com/security/advisory/Synology_SA_22_17	H-SYN-HD65-071122/4715
Out-of-bounds Read	20-Oct-2022	7.5	A vulnerability regarding out-of-bounds read is found in the session processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to obtain sensitive information via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected:	https://www.synology.com/security/advisory/Synology_SA_22_17	H-SYN-HD65-071122/4716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DS3622xs+, FS3410, and HD6500. **CVE ID : CVE-2022-3576**		
Vendor: Tenda					
Product: 11n					
Affected Version(s): -					
Improper Authentication	20-Oct-2022	9.8	Tenda 11N with firmware version V5.07.33_cn suffers from an Authentication Bypass vulnerability. **CVE ID : CVE-2022-42233**	N/A	H-TEN-11N-071122/4717
Product: ac10					
Affected Version(s): -					
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/fromNatStaticSetting. **CVE ID : CVE-2022-42163**	N/A	H-TEN-AC10-071122/4718
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/formSetClientState. **CVE ID : CVE-2022-42164**	N/A	H-TEN-AC10-071122/4719
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/formSetDeviceName.	N/A	H-TEN-AC10-071122/4720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42165		
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/formSetSpeedWan. **CVE ID : CVE-2022-42166**	N/A	H-TEN-AC10-071122/4721
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/formSetFirewallCfg. **CVE ID : CVE-2022-42167**	N/A	H-TEN-AC10-071122/4722
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/fromSetIpMacBind. **CVE ID : CVE-2022-42168**	N/A	H-TEN-AC10-071122/4723
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/addWifiMacFilter. **CVE ID : CVE-2022-42169**	N/A	H-TEN-AC10-071122/4724
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/formWifiWpsStart.	N/A	H-TEN-AC10-071122/4725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42170		
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/saveParentControlInfo. **CVE ID : CVE-2022-42171**	N/A	H-TEN-AC10-071122/4726
Product: ac15					
Affected Version(s): -					
Out-of-bounds Write	18-Oct-2022	7.5	Tenda AC15 V15.03.05.18 was discovered to contain a stack overflow via the timeZone parameter in the form_fast_setting_wifi_set function. **CVE ID : CVE-2022-43259**	N/A	H-TEN-AC15-071122/4727
Product: ac18					
Affected Version(s): -					
Out-of-bounds Write	18-Oct-2022	9.8	Tenda AC18 V15.03.05.19(6318) was discovered to contain a stack overflow via the time parameter in the fromSetSysTime function. **CVE ID : CVE-2022-43260**	N/A	H-TEN-AC18-071122/4728
Product: ax1803					
Affected Version(s): -					
Out-of-bounds Write	27-Oct-2022	9.8	In Tenda ax1803 v1.0.0.1, the http requests handled by the fromAdvSetMacMtuWan	N/A	H-TEN-AX18-071122/4729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functions, wanSpeed, cloneType, mac, can cause a stack overflow and enable remote code execution (RCE). **CVE ID : CVE-2022-40876**		
Out-of-bounds Write	27-Oct-2022	7.5	Tenda AX1803 v1.0.0.1 was discovered to contain a heap overflow vulnerability in the GetParentControlInfo function, which can cause a denial of service attack through a carefully constructed http request. **CVE ID : CVE-2022-40874**	N/A	H-TEN-AX18-071122/4730
Out-of-bounds Write	27-Oct-2022	7.5	Tenda AX1803 v1.0.0.1 was discovered to contain a heap overflow in the function GetParentControlInfo. **CVE ID : CVE-2022-40875**	N/A	H-TEN-AX18-071122/4731
Product: tx3					
Affected Version(s): -					
Out-of-bounds Write	19-Oct-2022	9.8	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the list parameter at /goform/SetVirtualServerCfg. **CVE ID : CVE-2022-43024**	N/A	H-TEN-TX3-071122/4732
Out-of-bounds Write	19-Oct-2022	9.8	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a	N/A	H-TEN-TX3-071122/4733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stack overflow via the startIp parameter at /goform/SetPptpServerCfg. **CVE ID : CVE-2022-43025**		
Out-of-bounds Write	19-Oct-2022	9.8	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the endIp parameter at /goform/SetPptpServerCfg. **CVE ID : CVE-2022-43026**	N/A	H-TEN-TX3-071122/4734
Out-of-bounds Write	19-Oct-2022	9.8	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the firewallEn parameter at /goform/SetFirewallCfg. **CVE ID : CVE-2022-43027**	N/A	H-TEN-TX3-071122/4735
Out-of-bounds Write	19-Oct-2022	9.8	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the timeZone parameter at /goform/SetSysTimeCfg. **CVE ID : CVE-2022-43028**	N/A	H-TEN-TX3-071122/4736
Out-of-bounds Write	19-Oct-2022	9.8	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the time parameter at /goform/SetSysTimeCfg.	N/A	H-TEN-TX3-071122/4737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43029		
Vendor: Tp-link					
Product: ax10					
Affected Version(s): 1.0					
Authentication Bypass by Capture-replay	18-Oct-2022	8.1	TP-Link AX10v1 V1_211117 allows attackers to execute a replay attack by using a previously transmitted encrypted authentication message and valid authentication token. Attackers are able to login to the web application as an admin user. **CVE ID : CVE-2022-41541**	https://www.tp-link.com/us/support/download/archer-ax10/v1/#Firmware	H-TP--AX10-071122/4738
Use of Hard-coded Credentials	18-Oct-2022	5.9	The web app client of TP-Link AX10v1 V1_211117 uses hard-coded cryptographic keys when communicating with the router. Attackers who are able to intercept the communications between the web client and router through a man-in-the-middle attack can then obtain the sequence key via a brute-force attack, and access sensitive information. **CVE ID : CVE-2022-41540**	https://www.tp-link.com/us/support/download/archer-ax10/v1/#Firmware	H-TP--AX10-071122/4739
Product: tl-wr841n					
Affected Version(s): 8.0					
Improper Neutralization of	18-Oct-2022	6.1	TP-Link TL-WR841N 8.0 4.17.16 Build 120201 Rel.54750n is vulnerable	N/A	H-TP--TL-W-071122/4740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			to Cross Site Scripting (XSS). **CVE ID : CVE-2022-42202**		
Vendor: Wago					
Product: 750-8100					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4741
Product: 750-8101					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8101\/000-010					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4743
Product: 750-8101\/025-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8102					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4745
Product: 750-8102\/025-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter.	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3281		
Product: 750-8202\/000-011					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4747
Product: 750-8202\/000-012					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4748
Product: 750-8202\/000-022					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4749
Product: 750-8202\/040-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4750
Product: 750-8206					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series	https://cert.vde.com/en/	H-WAG-750--071122/4751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	advisories/VDE-2022-042/	
Product: 750-8206\/025-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4752
Product: 750-8206\/025-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8206\/040-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4754
Product: 750-8206\/040-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8207					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4756
Product: 750-8207\/025-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8207\/025-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4758
Product: 750-8208					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8208\/025-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4760
Product: 750-8208\/025-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter.	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3281		
Product: 750-8210					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4762
Product: 750-8210\/025-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4763
Product: 750-8210\/040-000					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4764
Product: 750-8211					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4765
Product: 750-8211\/040-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series	https://cert.vde.com/en/	H-WAG-750--071122/4766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	advisories/VDE-2022-042/	
Product: 750-8212					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4767
Product: 750-8212\/000-100					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8212\/025-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4769
Product: 750-8212\/025-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8212\/025-002					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4771
Product: 750-8212\/040-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8212\/040-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4773
Product: 750-8212\/040-010					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8213					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4775
Product: 750-8213\/040-010					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter.	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3281		
Product: 750-8214					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4777
Product: 750-8215					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4778
Product: 750-8216					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4779
Product: 750-8216\/025-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4780
Product: 750-8216\/025-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series	https://cert.vde.com/en/	H-WAG-750--071122/4781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	advisories/VDE-2022-042/	
Product: 750-8216\/040-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4782
Product: 750-8217					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8217\/025-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4784
Product: 750-8217\/600-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8217\/625-000					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-750--071122/4786
Product: 751-9301					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-751--071122/4787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 752-8303\/8000-002					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-752--071122/4788
Product: 762-4101					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-4102					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4790
Product: 762-4103					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter.	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3281		
Product: 762-4104					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4792
Product: 762-4201\/8000-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4793
Product: 762-4202\/8000-001					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4794
Product: 762-4203\/8000-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4795
Product: 762-4204\/8000-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series	https://cert.vde.com/en/	H-WAG-762--071122/4796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	advisories/VDE-2022-042/	
Product: 762-4205\/8000-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4797
Product: 762-4206\/8000-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-4301\/8000-002					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4799
Product: 762-4302\/8000-002					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-4303\/8000-002					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4801
Product: 762-4304\/8000-002					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-5203\/8000-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4803
Product: 762-5204\/8000-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-5205\/8000-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4805
Product: 762-5206\/8000-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter.	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3281		
Product: 762-5303\/8000-002					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4807
Product: 762-5304\/8000-002					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4808
Product: 762-5305\/8000-002					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4809
Product: 762-5306\/8000-002					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4810
Product: 762-6201\/8000-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series	https://cert.vde.com/en/	H-WAG-762--071122/4811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	advisories/VDE-2022-042/	
Product: 762-6202\/8000-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4812
Product: 762-6203\/8000-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-6204\/8000-001					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4814
Product: 762-6301\/8000-002					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-6302\/8000-002					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4816
Product: 762-6303\/8000-002					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-6304\/8000-002					
Affected Version(s): -					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	H-WAG-762--071122/4818
Operating System					
Vendor: Acer					
Product: altos_w2000h-w570h_f4_firmware					
Affected Version(s): r01.03.0018					
Out-of-bounds Write	19-Oct-2022	9.8	Acer Altos W2000h-W570h F4 R01.03.0018 was discovered to contain a stack overflow in the RevserveMem component. This vulnerability allows attackers to cause a Denial of Service (DoS) via injecting crafted	http://acer.com	O-ACE-ALTO-071122/4819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			shellcode into the NVRAM variable. **CVE ID : CVE-2022-41415**		
Vendor: Apple					
Product: macos					
Affected Version(s): -					
Out-of-bounds Read	25-Oct-2022	7.8	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38436**	https://helpx.adobe.com/security/products/illustrator/apsb22-56.html	O-APP-MACO-071122/4820
Improper Input Validation	25-Oct-2022	7.8	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction	https://helpx.adobe.com/security/products/illustrator/apsb22-56.html	O-APP-MACO-071122/4821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in that a victim must open a malicious file. **CVE ID : CVE-2022-38435**		
Improper Privilege Management	17-Oct-2022	7.3	An attacker can pre-create the `/Applications/Google\ Drive.app/Contents/MacOS` directory which is expected to be owned by root to be owned by a non-root user. When the Drive for Desktop installer is run for the first time, it will place a binary in that directory with execute permissions and set its setuid bit. Since the attacker owns the directory, the attacker can replace the binary with a symlink, causing the installer to set the setuid bit on the symlink. When the symlink is executed, it will run with root permissions. We recommend upgrading past version 64.0 **CVE ID : CVE-2022-3421**	https://support.google.com/a/answer/7577057?hl=en	O-APP-MACO-071122/4822
Vendor: Asus					
Product: rt-n12e_firmware					
Affected Version(s): 2.0.0.39					
Missing Authentication for Critical Function	19-Oct-2022	7.5	Asus RT-N12E 2.0.0.39 is affected by an incorrect access control vulnerability. Through system.asp / start_apply.htm, an attacker can change the	https://www.asus.com/Networking/RTN12E/HelpDesk_BIOS/	O-ASU-RT-N-071122/4823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator password without any authentication. **CVE ID : CVE-2020-23648**		
Vendor: bosch					
Product: videojet_multi_4000_firmware					
Affected Version(s): * Up to (including) 6.31.0010					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2022	4.8	Incomplete filtering of JavaScript code in different configuration fields of the web based interface of the VIDEOJET multi 4000 allows an attacker with administrative credentials to store JavaScript code which will be executed for all administrators accessing the same configuration option. **CVE ID : CVE-2022-40184**	https://psirt.bosch.com/security-advisories/bosch-sa-454166-bt.html	O-BOS-VIDE-071122/4824
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2022	4.7	An error in the URL handler of the VIDEOJET multi 4000 may lead to a reflected cross site scripting (XSS) in the web-based interface. An attacker with knowledge of the encoder address can send a crafted link to a user, which will execute JavaScript code in the context of the user. **CVE ID : CVE-2022-40183**	https://psirt.bosch.com/security-advisories/bosch-sa-454166-bt.html	O-BOS-VIDE-071122/4825
Vendor: Broadcom					
Product: fabric_operating_system					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 7.4.2.j					
N/A	25-Oct-2022	8.8	A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, 7.4.2.j could allow a remote authenticated attacker to perform stack buffer overflow using in "firmwaredownload" and "diagshow" commands. **CVE ID : CVE-2022-33183**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2085	O-BRO-FABR-071122/4826
Out-of-bounds Write	25-Oct-2022	7.8	A vulnerability in fab_seg.c.h libraries of all Brocade Fabric OS versions before Brocade Fabric OS v9.1.1, v9.0.1e, v8.2.3c, v8.2.0_cbn5, 7.4.2j could allow local authenticated attackers to exploit stack-based buffer overflows and execute arbitrary code as the root user account. **CVE ID : CVE-2022-33184**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2080	O-BRO-FABR-071122/4827
Exposure of Sensitive Information to an Unauthorized Actor	25-Oct-2022	5.5	An information disclosure vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, 7.4.2.j could allow a local authenticated attacker to read sensitive files using switch commands "configshow" and "supportlink". **CVE ID : CVE-2022-33181**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2083	O-BRO-FABR-071122/4828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 7.4.2j					
N/A	25-Oct-2022	8.8	A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, and 7.4.2j could allow a local authenticated user to break out of restricted shells with “set context” and escalate privileges. **CVE ID : CVE-2022-33179**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2079	O-BRO-FABR-071122/4829
Insecure Storage of Sensitive Information	25-Oct-2022	6.5	Brocade Fabric OS Web Application services before Brocade Fabric v9.1.0, v9.0.1e, v8.2.3c, v7.4.2j store server and user passwords in the debug statements. This could allow a local user to extract the passwords from a debug file. **CVE ID : CVE-2022-28170**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2076	O-BRO-FABR-071122/4830
Affected Version(s): * Up to (excluding) 9.0.0					
Improper Input Validation	25-Oct-2022	7.2	A vulnerability in the radius authentication system of Brocade Fabric OS before Brocade Fabric OS 9.0 could allow a remote attacker to execute arbitrary code on the Brocade switch. **CVE ID : CVE-2022-33178**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2077	O-BRO-FABR-071122/4831
Affected Version(s): * Up to (excluding) 9.0.1e					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	25-Oct-2022	7.8	Several commands in Brocade Fabric OS before Brocade Fabric OS v.9.0.1e, and v9.1.0 use unsafe string functions to process user input. Authenticated local attackers could abuse these vulnerabilities to exploit stack-based buffer overflows, allowing arbitrary code execution as the root user account. **CVE ID : CVE-2022-33185**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2078	O-BRO-FABR-071122/4832
Affected Version(s): 9.1.0					
N/A	25-Oct-2022	8.8	A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, and 7.4.2j could allow a local authenticated user to break out of restricted shells with “set context” and escalate privileges. **CVE ID : CVE-2022-33179**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2079	O-BRO-FABR-071122/4833
N/A	25-Oct-2022	8.8	A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, 7.4.2.j could allow a remote authenticated attacker to perform stack buffer overflow using in “firmwaredownload” and “diagshow” commands. **CVE ID : CVE-2022-33183**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2085	O-BRO-FABR-071122/4834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Oct-2022	7.8	A privilege escalation vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, could allow a local authenticated user to escalate its privilege to root using switch commands “supportlink”, “firmwaredownload”, “portcfgupload, license, and “fosexec”. **CVE ID : CVE-2022-33182**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2084	O-BRO-FABR-071122/4835
Out-of-bounds Write	25-Oct-2022	7.8	Several commands in Brocade Fabric OS before Brocade Fabric OS v.9.0.1e, and v9.1.0 use unsafe string functions to process user input. Authenticated local attackers could abuse these vulnerabilities to exploit stack-based buffer overflows, allowing arbitrary code execution as the root user account. **CVE ID : CVE-2022-33185**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2078	O-BRO-FABR-071122/4836
Insecure Storage of Sensitive Information	25-Oct-2022	6.5	Brocade Fabric OS Web Application services before Brocade Fabric v9.1.0, v9.0.1e, v8.2.3c, v7.4.2j store server and user passwords in the debug statements. This could allow a local user to extract the passwords from a debug file.	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-	O-BRO-FABR-071122/4837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28170	advisory-2022-2076	
N/A	25-Oct-2022	5.5	A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5 could allow a local authenticated attacker to export out sensitive files with "seccryptocfg", "configupload". **CVE ID : CVE-2022-33180**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2079	O-BRO-FABR-071122/4838
Exposure of Sensitive Information to an Unauthorized Actor	25-Oct-2022	5.5	An information disclosure vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, 7.4.2.j could allow a local authenticated attacker to read sensitive files using switch commands "configshow" and "supportlink". **CVE ID : CVE-2022-33181**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2083	O-BRO-FABR-071122/4839
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.2.3c					
Improper Privilege Management	25-Oct-2022	8.8	Brocade Webtools in Brocade Fabric OS versions before Brocade Fabric OS versions v9.1.1, v9.0.1e, and v8.2.3c could allow a low privilege webtools, user, to gain elevated admin rights, or privileges, beyond what is intended or entitled for that user. By exploiting this vulnerability, a user	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2075	O-BRO-FABR-071122/4840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			whose role is not an admin can create a new user with an admin role using the operator session id. The issue was replicated after intercepting the admin, and operator authorization headers sent unencrypted and editing a user addition request to use the operator's authorization header. **CVE ID : CVE-2022-28169**		
N/A	25-Oct-2022	8.8	A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, and 7.4.2j could allow a local authenticated user to break out of restricted shells with “set context” and escalate privileges. **CVE ID : CVE-2022-33179**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2079	O-BRO-FABR-071122/4841
N/A	25-Oct-2022	8.8	A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, 7.4.2.j could allow a remote authenticated attacker to perform stack buffer overflow using in “firmwaredownload” and “diagshow” commands. **CVE ID : CVE-2022-33183**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2085	O-BRO-FABR-071122/4842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Oct-2022	7.8	A privilege escalation vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, could allow a local authenticated user to escalate its privilege to root using switch commands “supportlink”, “firmwaredownload”, “portcfgupload, license, and “fosexec”. **CVE ID : CVE-2022-33182**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2084	O-BRO-FABR-071122/4843
Out-of-bounds Write	25-Oct-2022	7.8	A vulnerability in fab_seg.c.h libraries of all Brocade Fabric OS versions before Brocade Fabric OS v9.1.1, v9.0.1e, v8.2.3c, v8.2.0_cbn5, 7.4.2j could allow local authenticated attackers to exploit stack-based buffer overflows and execute arbitrary code as the root user account. **CVE ID : CVE-2022-33184**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2080	O-BRO-FABR-071122/4844
Insecure Storage of Sensitive Information	25-Oct-2022	6.5	Brocade Fabric OS Web Application services before Brocade Fabric v9.1.0, v9.0.1e, v8.2.3c, v7.4.2j store server and user passwords in the debug statements. This could allow a local user to extract the passwords from a debug file. **CVE ID : CVE-2022-28170**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2076	O-BRO-FABR-071122/4845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Oct-2022	5.5	A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5 could allow a local authenticated attacker to export out sensitive files with "seccryptocfg", "configupload". **CVE ID : CVE-2022-33180**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2079	O-BRO-FABR-071122/4846
Exposure of Sensitive Information to an Unauthorized Actor	25-Oct-2022	5.5	An information disclosure vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, 7.4.2.j could allow a local authenticated attacker to read sensitive files using switch commands "configshow" and "supportlink". **CVE ID : CVE-2022-33181**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2083	O-BRO-FABR-071122/4847
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.0.1e					
Improper Privilege Management	25-Oct-2022	8.8	Brocade Webtools in Brocade Fabric OS versions before Brocade Fabric OS versions v9.1.1, v9.0.1e, and v8.2.3c could allow a low privilege webtools, user, to gain elevated admin rights, or privileges, beyond what is intended or entitled for that user. By exploiting this vulnerability, a user whose role is not an admin can create a new	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2075	O-BRO-FABR-071122/4848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user with an admin role using the operator session id. The issue was replicated after intercepting the admin, and operator authorization headers sent unencrypted and editing a user addition request to use the operator's authorization header. **CVE ID : CVE-2022-28169**		
N/A	25-Oct-2022	8.8	A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, and 7.4.2j could allow a local authenticated user to break out of restricted shells with “set context” and escalate privileges. **CVE ID : CVE-2022-33179**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2079	O-BRO-FABR-071122/4849
N/A	25-Oct-2022	8.8	A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, 7.4.2.j could allow a remote authenticated attacker to perform stack buffer overflow using in “firmwaredownload” and “diagshow” commands. **CVE ID : CVE-2022-33183**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2085	O-BRO-FABR-071122/4850
N/A	25-Oct-2022	7.8	A privilege escalation vulnerability in Brocade Fabric OS CLI before	https://www.broadcom.com/suppor	O-BRO-FABR-071122/4851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, could allow a local authenticated user to escalate its privilege to root using switch commands “supportlink”, “firmwaredownload”, “portcfgupload, license, and “fosexec”. **CVE ID : CVE-2022-33182**	t/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2084	
Out-of-bounds Write	25-Oct-2022	7.8	A vulnerability in fab_seg.c.h libraries of all Brocade Fabric OS versions before Brocade Fabric OS v9.1.1, v9.0.1e, v8.2.3c, v8.2.0_cbn5, 7.4.2j could allow local authenticated attackers to exploit stack-based buffer overflows and execute arbitrary code as the root user account. **CVE ID : CVE-2022-33184**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2080	O-BRO-FABR-071122/4852
Insecure Storage of Sensitive Information	25-Oct-2022	6.5	Brocade Fabric OS Web Application services before Brocade Fabric v9.1.0, v9.0.1e, v8.2.3c, v7.4.2j store server and user passwords in the debug statements. This could allow a local user to extract the passwords from a debug file. **CVE ID : CVE-2022-28170**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2076	O-BRO-FABR-071122/4853
N/A	25-Oct-2022	5.5	A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c,	https://www.broadcom.com/support/fibre-	O-BRO-FABR-071122/4854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.2.0cbn5 could allow a local authenticated attacker to export out sensitive files with "seccryptocfg", "configupload". **CVE ID : CVE-2022-33180**	channel-networking/security-advisories/brocade-security-advisory-2022-2079	
Exposure of Sensitive Information to an Unauthorized Actor	25-Oct-2022	5.5	An information disclosure vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, 7.4.2.j could allow a local authenticated attacker to read sensitive files using switch commands "configshow" and "supportlink". **CVE ID : CVE-2022-33181**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2083	O-BRO-FABR-071122/4855
Affected Version(s): From (including) 9.1.0 Up to (excluding) 9.1.1					
Improper Privilege Management	25-Oct-2022	8.8	Brocade Webtools in Brocade Fabric OS versions before Brocade Fabric OS versions v9.1.1, v9.0.1e, and v8.2.3c could allow a low privilege webtools, user, to gain elevated admin rights, or privileges, beyond what is intended or entitled for that user. By exploiting this vulnerability, a user whose role is not an admin can create a new user with an admin role using the operator session id. The issue was replicated after	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2075	O-BRO-FABR-071122/4856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intercepting the admin, and operator authorization headers sent unencrypted and editing a user addition request to use the operator's authorization header. **CVE ID : CVE-2022-28169**		
Vendor: Cisco					
Product: meraki_mx100_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx105_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx250_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-MERA-071122/4861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**	meraki-mx-vpn-dos-vnESbgBf	
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN	https://tools.cisco.com/s	O-CIS-MERA-071122/4862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability.	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20933		
Product: meraki_mx400_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx450_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx600_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx64w_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ci	O-CIS-MERA-071122/4869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**	sco-sa-meraki-mx-vpn-dos-vnESbgBf	
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx64_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx65w_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx65_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx67cw_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3	https://tools.cisco.com/security/center/content/	O-CIS-MERA-071122/4877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**	CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx67w_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx67_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx68cw_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx68w_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3	https://tools.cisco.com/security/center/content/	O-CIS-MERA-071122/4885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**	CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx68_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx75_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx84_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx85_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3	https://tools.cisco.com/security/center/content/	O-CIS-MERA-071122/4893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**	CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_mx95_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_vmx_firmware					
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.16.6					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.10.1					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_z3c_firmware					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf	O-CIS-MERA-071122/4899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**		
Product: meraki_z3_firmware					
Affected Version(s): -					
N/A	26-Oct-2022	8.6	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-	O-CIS-MERA-071122/4900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability. **CVE ID : CVE-2022-20933**	vpn-dos-vnESbgBf	
Product: roomos					
Affected Version(s): -					
Improper Limitation of a	26-Oct-2022	7.1	Multiple vulnerabilities in Cisco TelePresence Collaboration Endpoint	https://tools.cisco.com/security/cent	O-CIS-ROOM-071122/4901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			(CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive data, or write arbitrary files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20955**	er/content/CiscoSecurityAdvisory/cisco-sa-roomos-trav-beFvCcyu	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Oct-2022	7.1	Multiple vulnerabilities in Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive data, or write arbitrary files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20954**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-trav-beFvCcyu	O-CIS-ROOM-071122/4902
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Oct-2022	5.5	Multiple vulnerabilities in Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive data, or write arbitrary files on an affected device. For more information about these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-trav-beFvCcyu	O-CIS-ROOM-071122/4903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20953**		
Affected Version(s): * Up to (excluding) 10.15.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Oct-2022	7.2	Multiple vulnerabilities in Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive data, or write arbitrary files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20811**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-trav-beFvCcyu	O-CIS-ROOM-071122/4904
Affected Version(s): * Up to (excluding) 10.20.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Oct-2022	6.7	Multiple vulnerabilities in Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an attacker to conduct path traversal attacks, view sensitive data, or write arbitrary files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-trav-beFvCcyu	O-CIS-ROOM-071122/4905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: corsair					
Product: k63_firmware					
Affected Version(s): 3.1.3					
Missing Encryption of Sensitive Data	19-Oct-2022	6.8	Missing AES encryption in Corsair K63 Wireless 3.1.3 allows physically proximate attackers to inject and sniff keystrokes via 2.4 GHz radio transmissions. **CVE ID : CVE-2022-35860**	https://www.corsair.com/us/en/Categories/Products/Gaming-Keyboards/Wireless-Keyboards/K63-Wireless-Mechanical-Gaming-Keyboard-%E2%80%94-Blue-LED-%E2%80%94-CHERRY%C2%AE-MX-Red/p/CH-9145030-NA	O-COR-K63_-071122/4906
Vendor: Dell					
Product: emc_powerscale_onefs					
Affected Version(s): From (including) 9.1.0.0 Up to (including) 9.1.0.19					
Insertion of Sensitive Information into Log File	21-Oct-2022	4.4	Dell PowerScale OneFS, versions 9.0.0 up to and including 9.1.0.19, 9.2.1.12, and 9.3.0.6, contain sensitive data in log files vulnerability. A privileged local user may potentially exploit this vulnerability, leading to disclosure of this sensitive data. **CVE ID : CVE-2022-31239**	https://www.dell.com/support/kbdoc/en-us/000201094/dsa-2022-149-dell-emc-powerscale-onefs-security-update?lang=en	O-DEL-EMC_-071122/4907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 9.1.0.0 Up to (including) 9.1.0.21					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-2022	6.7	Dell PowerScale OneFS, versions 8.2.2-9.3.0, contain an OS command injection vulnerability. A privileged local malicious user could potentially exploit this vulnerability, leading to a full system compromise. This impacts compliance mode clusters. **CVE ID : CVE-2022-34437**	https://www.dell.com/support/kbdoc/en-us/000204053/dsa-2022-245-dell-emc-powerscale-onefs-security-update-for-multiple-security-updates	O-DEL-EMC_-071122/4908
Affected Version(s): From (including) 9.1.0.0 Up to (including) 9.1.0.22					
Allocation of Resources Without Limits or Throttling	21-Oct-2022	7.5	Dell PowerScale OneFS, versions 8.2.0.x-9.4.0.x contain allocation of Resources Without Limits or Throttling vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to denial of service and performance issue on that node. **CVE ID : CVE-2022-34439**	https://www.dell.com/support/kbdoc/en-us/000204053/dsa-2022-245-dell-emc-powerscale-onefs-security-update-for-multiple-security-updates	O-DEL-EMC_-071122/4909
Improper Privilege Management	21-Oct-2022	6.7	Dell PowerScale OneFS, versions 8.2.x-9.4.0.x, contain a privilege context switching error. A local authenticated malicious user with high privileges could potentially exploit this vulnerability, leading to full system compromise.	https://www.dell.com/support/kbdoc/en-us/000204053/dsa-2022-245-dell-emc-powerscale-onefs-security-	O-DEL-EMC_-071122/4910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This impacts compliance mode clusters. **CVE ID : CVE-2022-34438**	update-for-multiple-security-updates	
Affected Version(s): From (including) 9.2.1.0 Up to (including) 9.2.1.12					
Insertion of Sensitive Information into Log File	21-Oct-2022	4.4	Dell PowerScale OneFS, versions 9.0.0 up to and including 9.1.0.19, 9.2.1.12, and 9.3.0.6, contain sensitive data in log files vulnerability. A privileged local user may potentially exploit this vulnerability, leading to disclosure of this sensitive data. **CVE ID : CVE-2022-31239**	https://www.dell.com/support/kbdoc/en-us/000201094/dsa-2022-149-dell-emc-powerscale-onefs-security-update?lang=en	O-DEL-EMC_-071122/4911
Affected Version(s): From (including) 9.2.1.0 Up to (including) 9.2.1.15					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-2022	6.7	Dell PowerScale OneFS, versions 8.2.2-9.3.0, contain an OS command injection vulnerability. A privileged local malicious user could potentially exploit this vulnerability, leading to a full system compromise. This impacts compliance mode clusters. **CVE ID : CVE-2022-34437**	https://www.dell.com/support/kbdoc/en-us/000204053/dsa-2022-245-dell-emc-powerscale-onefs-security-update-for-multiple-security-updates	O-DEL-EMC_-071122/4912
Improper Privilege Management	21-Oct-2022	6.7	Dell PowerScale OneFS, versions 8.2.x-9.4.0.x, contain a privilege context switching error. A local authenticated malicious user with high privileges could potentially exploit this	https://www.dell.com/support/kbdoc/en-us/000204053/dsa-2022-245-dell-emc-	O-DEL-EMC_-071122/4913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, leading to full system compromise. This impacts compliance mode clusters. **CVE ID : CVE-2022-34438**	powerscale-onefs-security-update-for-multiple-security-updates	
Affected Version(s): From (including) 9.2.1.0 Up to (including) 9.2.1.16					
Allocation of Resources Without Limits or Throttling	21-Oct-2022	7.5	Dell PowerScale OneFS, versions 8.2.0.x-9.4.0.x contain allocation of Resources Without Limits or Throttling vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to denial of service and performance issue on that node. **CVE ID : CVE-2022-34439**	https://www.dell.com/support/kbdoc/en-us/000204053/dsa-2022-245-dell-emc-powerscale-onefs-security-update-for-multiple-security-updates	O-DEL-EMC_-071122/4914
Affected Version(s): From (including) 9.3.0.0 Up to (including) 9.3.0.6					
Insertion of Sensitive Information into Log File	21-Oct-2022	4.4	Dell PowerScale OneFS, versions 9.0.0 up to and including 9.1.0.19, 9.2.1.12, and 9.3.0.6, contain sensitive data in log files vulnerability. A privileged local user may potentially exploit this vulnerability, leading to disclosure of this sensitive data. **CVE ID : CVE-2022-31239**	https://www.dell.com/support/kbdoc/en-us/000201094/dsa-2022-149-dell-emc-powerscale-onefs-security-update?lang=en	O-DEL-EMC_-071122/4915
Affected Version(s): From (including) 9.3.0.0 Up to (including) 9.3.0.7					
Allocation of Resources Without	21-Oct-2022	7.5	Dell PowerScale OneFS, versions 8.2.0.x-9.4.0.x contain allocation of Resources Without	https://www.dell.com/support/kbdoc/en-	O-DEL-EMC_-071122/4916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			Limits or Throttling vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to denial of service and performance issue on that node. **CVE ID : CVE-2022-34439**	us/000204053/dsa-2022-245-dell-emc-powerscale-onefs-security-update-for-multiple-security-updates	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-2022	6.7	Dell PowerScale OneFS, versions 8.2.2-9.3.0, contain an OS command injection vulnerability. A privileged local malicious user could potentially exploit this vulnerability, leading to a full system compromise. This impacts compliance mode clusters. **CVE ID : CVE-2022-34437**	https://www.dell.com/support/kbdoc/en-us/000204053/dsa-2022-245-dell-emc-powerscale-onefs-security-update-for-multiple-security-updates	O-DEL-EMC_-071122/4917
Improper Privilege Management	21-Oct-2022	6.7	Dell PowerScale OneFS, versions 8.2.x-9.4.0.x, contain a privilege context switching error. A local authenticated malicious user with high privileges could potentially exploit this vulnerability, leading to full system compromise. This impacts compliance mode clusters. **CVE ID : CVE-2022-34438**	https://www.dell.com/support/kbdoc/en-us/000204053/dsa-2022-245-dell-emc-powerscale-onefs-security-update-for-multiple-security-updates	O-DEL-EMC_-071122/4918
Affected Version(s): From (including) 9.4.0.0 Up to (including) 9.4.0.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	21-Oct-2022	7.5	Dell PowerScale OneFS, versions 8.2.0.x-9.4.0.x contain allocation of Resources Without Limits or Throttling vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to denial of service and performance issue on that node. **CVE ID : CVE-2022-34439**	https://www.dell.com/support/kbdoc/en-us/000204053/dsa-2022-245-dell-emc-powerscale-onefs-security-update-for-multiple-security-updates	O-DEL-EMC_-071122/4919
Improper Privilege Management	21-Oct-2022	6.7	Dell PowerScale OneFS, versions 8.2.x-9.4.0.x, contain a privilege context switching error. A local authenticated malicious user with high privileges could potentially exploit this vulnerability, leading to full system compromise. This impacts compliance mode clusters. **CVE ID : CVE-2022-34438**	https://www.dell.com/support/kbdoc/en-us/000204053/dsa-2022-245-dell-emc-powerscale-onefs-security-update-for-multiple-security-updates	O-DEL-EMC_-071122/4920
Product: powerstoreos					
Affected Version(s): 2.1.0.0					
Improper Authentication	21-Oct-2022	9.8	Dell PowerStore versions 2.1.0.x contain an Authentication bypass vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability under specific configuration. An attacker would gain	https://www.dell.com/support/kbdoc/000196367	O-DEL-POWE-071122/4921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access upon successful exploit. **CVE ID : CVE-2022-26870**		
Affected Version(s): 2.1.0.1					
Improper Authentication	21-Oct-2022	9.8	Dell PowerStore versions 2.1.0.x contain an Authentication bypass vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability under specific configuration. An attacker would gain unauthorized access upon successful exploit. **CVE ID : CVE-2022-26870**	https://www.dell.com/support/kbdoc/000196367	O-DEL-POWE-071122/4922
Vendor: Dlink					
Product: dir-816_firmware					
Affected Version(s): 1.10b05					
Out-of-bounds Write	26-Oct-2022	9.8	D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the srcip parameter at /goform/form2IPQoSTcAdd. **CVE ID : CVE-2022-42998**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--071122/4923
Out-of-bounds Write	26-Oct-2022	9.8	D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the wizardstep4_pskpwd parameter at /goform/form2WizardStep4. **CVE ID : CVE-2022-43000**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--071122/4924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	26-Oct-2022	9.8	D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the pskValue parameter in the setSecurity function. **CVE ID : CVE-2022-43001**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--071122/4925
Out-of-bounds Write	26-Oct-2022	9.8	D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the wizardstep54_pskpwd parameter at /goform/form2WizardStep54. **CVE ID : CVE-2022-43002**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--071122/4926
Out-of-bounds Write	26-Oct-2022	9.8	D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the pskValue parameter in the setRepeaterSecurity function. **CVE ID : CVE-2022-43003**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--071122/4927
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Oct-2022	7.5	D-Link DIR-816 A2 1.10 B05 was discovered to contain multiple command injection vulnerabilities via the admuser and admpass parameters at /goform/setSysAdm. **CVE ID : CVE-2022-42999**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--071122/4928
Product: dir-878_firmware					
Affected Version(s): 1.30b08					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Oct-2022	9.8	D-Link DIR878 1.30B08 Hotfix_04 was discovered to contain a command injection vulnerability via the component /bin/proc.cgi. **CVE ID : CVE-2022-43184**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--071122/4929
Vendor: F5					
Product: f5os-a					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.1.0					
Improper Privilege Management	19-Oct-2022	8.8	In F5OS-A version 1.x before 1.1.0 and F5OS-C version 1.x before 1.5.0, excessive file permissions in F5OS allows an authenticated local attacker to execute limited set of commands in a container and impact the F5OS controller. **CVE ID : CVE-2022-41835**	https://support.f5.com/csp/article/K33484483	O-F5-F5OS-071122/4930
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Oct-2022	5.5	In F5OS-A version 1.x before 1.1.0 and F5OS-C version 1.x before 1.4.0, a directory traversal vulnerability exists in an undisclosed location of the F5OS CLI that allows an attacker to read arbitrary files. **CVE ID : CVE-2022-41780**	https://support.f5.com/csp/article/K81701735	O-F5-F5OS-071122/4931
Product: f5os-c					
Affected Version(s): From (excluding) 1.1.0 Up to (excluding) 1.4.0					
Improper Limitation of a	19-Oct-2022	5.5	In F5OS-A version 1.x before 1.1.0 and F5OS-C version 1.x before 1.4.0, a	https://support.f5.com/c	O-F5-F5OS-071122/4932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			directory traversal vulnerability exists in an undisclosed location of the F5OS CLI that allows an attacker to read arbitrary files. **CVE ID : CVE-2022-41780**	sp/article/K81701735	
Affected Version(s): From (excluding) 1.3.0 Up to (excluding) 1.5.0					
Improper Privilege Management	19-Oct-2022	8.8	In F5OS-A version 1.x before 1.1.0 and F5OS-C version 1.x before 1.5.0, excessive file permissions in F5OS allows an authenticated local attacker to execute limited set of commands in a container and impact the F5OS controller. **CVE ID : CVE-2022-41835**	https://support.f5.com/csp/article/K33484483	O-F5-F5OS-071122/4933
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 36					
Integer Underflow (Wrap or Wraparound)	17-Oct-2022	6.5	An integer underflow issue was found in the QEMU VNC server while processing ClientCutText messages in the extended format. A malicious client could use this flaw to make QEMU unresponsive by sending a specially crafted payload message, resulting in a denial of service. **CVE ID : CVE-2022-3165**	https://gitlab.com/qemu-project/qemu/-/commit/d307040b18	O-FED-FEDO-071122/4934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	29-Oct-2022	0	curl before 7.86.0 has a double free. If curl is told to use an HTTP proxy for a transfer with a non-HTTP(S) URL, it sets up the connection to the remote server by issuing a CONNECT request to the proxy, and then tunnels the rest of the protocol through. An HTTP proxy might refuse this request (HTTP proxies often only allow outgoing connections to specific port numbers, like 443 for HTTPS) and instead return a non-200 status code to the client. Due to flaws in the error/cleanup handling, this could trigger a double free in curl if one of the following schemes were used in the URL for the transfer: dict, gopher, gophers, ldap, ldaps, rtmp, rtmps, or telnet. The earliest affected version is 7.77.0. **CVE ID : CVE-2022-42915**	N/A	O-FED-FEDO-071122/4935
Vendor: Fortinet					
Product: fortios					
Affected Version(s): 7.2.0					
Access of Uninitialized Pointer	18-Oct-2022	7.5	A access of uninitialized pointer in Fortinet FortiOS version 7.2.0, 7.0.0 through 7.0.5, 6.4.0 through 6.4.8, 6.2.0 through 6.2.10, 6.0.x, FortiProxy version 7.0.0	https://fortiguard.com/psirt/FG-IR-22-086	O-FOR-FORT-071122/4936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 7.0.4, 2.0.0 through 2.0.9, 1.2.x allows a remote unauthenticated or authenticated attacker to crash the sslvpn daemon via an HTTP GET request. **CVE ID : CVE-2022-29055**		
Affected Version(s): From (including) 6.2.0 Up to (excluding) 6.2.11					
Access of Uninitialized Pointer	18-Oct-2022	7.5	A access of uninitialized pointer in Fortinet FortiOS version 7.2.0, 7.0.0 through 7.0.5, 6.4.0 through 6.4.8, 6.2.0 through 6.2.10, 6.0.x, FortiProxy version 7.0.0 through 7.0.4, 2.0.0 through 2.0.9, 1.2.x allows a remote unauthenticated or authenticated attacker to crash the sslvpn daemon via an HTTP GET request. **CVE ID : CVE-2022-29055**	https://fortiguard.com/psirt/FG-IR-22-086	O-FOR-FORT-071122/4937
Affected Version(s): From (including) 6.4.0 Up to (excluding) 6.4.10					
Access of Uninitialized Pointer	18-Oct-2022	7.5	A access of uninitialized pointer in Fortinet FortiOS version 7.2.0, 7.0.0 through 7.0.5, 6.4.0 through 6.4.8, 6.2.0 through 6.2.10, 6.0.x, FortiProxy version 7.0.0 through 7.0.4, 2.0.0 through 2.0.9, 1.2.x allows a remote unauthenticated or authenticated attacker to crash the sslvpn daemon via an HTTP GET request.	https://fortiguard.com/psirt/FG-IR-22-086	O-FOR-FORT-071122/4938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29055		
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.7					
Missing Authentication for Critical Function	18-Oct-2022	9.8	An authentication bypass using an alternate path or channel [CWE-288] in Fortinet FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0 allows an unauthenticated atttacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests. **CVE ID : CVE-2022-40684**	https://fortiguard.com/psirt/FG-IR-22-377	O-FOR-FORT-071122/4939
Access of Uninitialized Pointer	18-Oct-2022	7.5	A access of uninitialized pointer in Fortinet FortiOS version 7.2.0, 7.0.0 through 7.0.5, 6.4.0 through 6.4.8, 6.2.0 through 6.2.10, 6.0.x, FortiProxy version 7.0.0 through 7.0.4, 2.0.0 through 2.0.9, 1.2.x allows a remote unauthenticated or authenticated attacker to crash the sslvpn daemon via an HTTP GET request. **CVE ID : CVE-2022-29055**	https://fortiguard.com/psirt/FG-IR-22-086	O-FOR-FORT-071122/4940
Affected Version(s): From (including) 7.2.0 Up to (excluding) 7.2.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	18-Oct-2022	9.8	An authentication bypass using an alternate path or channel [CWE-288] in Fortinet FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0 allows an unauthenticated atttacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests. **CVE ID : CVE-2022-40684**	https://fortiguard.com/psirt/FG-IR-22-377	O-FOR-FORT-071122/4941
Vendor: gl-inet					
Product: gl-ax1800_firmware					
Affected Version(s): 3.214					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Oct-2022	8.8	gl-inet GL-MT300N-V2 Mango v3.212 and GL-AX1800 Flint v3.214 were discovered to contain multiple command injection vulnerabilities via the ping_addr and trace_addr function parameters. **CVE ID : CVE-2022-31898**	N/A	O-GL--GL-A-071122/4942
Product: gl-mt300n-v2_firmware					
Affected Version(s): 3.212					
Improper Neutralization of Special Elements	27-Oct-2022	8.8	gl-inet GL-MT300N-V2 Mango v3.212 and GL-AX1800 Flint v3.214 were discovered to contain multiple	N/A	O-GL--GL-M-071122/4943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			command injection vulnerabilities via the ping_addr and trace_addr function parameters. **CVE ID : CVE-2022-31898**		
Vendor: Goabode					
Product: iota_all-in-one_security_kit_firmware					
Affected Version(s): 6.9x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.9	Four OS command injection vulnerabilities exists in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability focuses on the unsafe use of the `ssid_hex` HTTP parameter to construct an OS Command at offset `0x19afc0` of the `/root/hpgw` binary included in firmware 6.9Z. **CVE ID : CVE-2022-33204**	N/A	O-GOA-IOTA-071122/4944
Improper Neutralization of Special Elements used in an	25-Oct-2022	9.9	Four OS command injection vulnerabilities exists in the web interface /action/wirelessConnect functionality of Abode	N/A	O-GOA-IOTA-071122/4945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability focuses on the unsafe use of the `wpapsk_hex` HTTP parameter to construct an OS Command at offset `0x19b0ac` of the `/root/hpgw` binary included in firmware 6.9Z. **CVE ID : CVE-2022-33205**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.9	Four OS command injection vulnerabilities exists in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability focuses on a second unsafe use of the `default_key_id` HTTP parameter to construct an OS Command at offset `0x19B234` of the	N/A	O-GOA-IOTA-071122/4946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`/root/hpgw` binary included in firmware 6.9Z. **CVE ID : CVE-2022-33207**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.9	Four OS command injection vulnerabilities exists in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability focuses on the unsafe use of the `key` and `default_key_id` HTTP parameters to construct an OS Command crafted at offset `0x19b1f4` of the `/root/hpgw` binary included in firmware 6.9Z. **CVE ID : CVE-2022-33206**	N/A	O-GOA-IOTA-071122/4947
Improper Access Control	25-Oct-2022	9.8	An authentication bypass vulnerability exists in the GHOME control functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted network request can lead to arbitrary XCMD execution. An attacker	N/A	O-GOA-IOTA-071122/4948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-27805**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.8	An OS command injection vulnerability exists in the web interface util_set_serial_mac functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-29472**	N/A	O-GOA-IOTA-071122/4949
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.8	An os command injection vulnerability exists in the web interface util_set_abode_code functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-27804**	N/A	O-GOA-IOTA-071122/4950
Use of Hard-coded	25-Oct-2022	9.8	An authentication bypass vulnerability exists in the web interface /action/factory*	N/A	O-GOA-IOTA-071122/4951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Credentials			functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP header can lead to authentication bypass. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-29477**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.8	An OS command injection vulnerability exists in the XCMD setUPnP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to arbitrary command execution. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-30541**	N/A	O-GOA-IOTA-071122/4952
Use of Externally-Controlled Format String	25-Oct-2022	9.8	A format string injection vulnerability exists in the ghome_process_control_packet functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted XCMD can lead to memory corruption, information disclosure and denial of service. An attacker can send a malicious XML payload to trigger this vulnerability.	N/A	O-GOA-IOTA-071122/4953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33938		
Stack-based Buffer Overflow	25-Oct-2022	9.8	A stack-based buffer overflow vulnerability exists in the XCMD setIPCam functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to remote code execution. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-32454**	N/A	O-GOA-IOTA-071122/4954
Use of Externally-Controlled Format String	25-Oct-2022	9.8	A format string injection vulnerability exists in the XCMD getVarHA functionality of abode systems, inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to memory corruption, information disclosure, and denial of service. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-35244**	N/A	O-GOA-IOTA-071122/4955
Use of Externally-Controlled Format String	25-Oct-2022	9.8	Four format string injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. Specially-crafted	N/A	O-GOA-IOTA-071122/4956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration values can lead to memory corruption, information disclosure and denial of service. An attacker can modify a configuration value and then execute an XCMD to trigger these vulnerabilities.This vulnerability arises from format string injection via the `ssid` and `ssid_hex` configuration parameters, as used within the `testWifiAP` XCMD handler **CVE ID : CVE-2022-35874**		
Use of Externally-Controlled Format String	25-Oct-2022	9.8	Four format string injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. Specially-crafted configuration values can lead to memory corruption, information disclosure and denial of service. An attacker can modify a configuration value and then execute an XCMD to trigger these vulnerabilities.This vulnerability arises from format string injection via the `wpapsk` configuration parameter, as used within the `testWifiAP` XCMD handler	N/A	O-GOA-IOTA-071122/4957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35875		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.8	An OS command injection vulnerability exists in the XCMD doDebug functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to arbitrary command execution. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-32773**	N/A	O-GOA-IOTA-071122/4958
Use of Externally-Controlled Format String	25-Oct-2022	9.8	Four format string injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. Specially-crafted configuration values can lead to memory corruption, information disclosure and denial of service. An attacker can modify a configuration value and then execute an XCMD to trigger these vulnerabilities.This vulnerability arises from format string injection via the `default_key_id` and `key` configuration parameters, as used within the `testWifiAP` XCMD handler	N/A	O-GOA-IOTA-071122/4959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35876		
Use of Externally-Controlled Format String	25-Oct-2022	9.8	Four format string injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. Specially-crafted configuration values can lead to memory corruption, information disclosure and denial of service. An attacker can modify a configuration value and then execute an XCMD to trigger these vulnerabilities.This vulnerability arises from format string injection via the `default_key_id` configuration parameter, as used within the `testWifiAP` XCMD handler **CVE ID : CVE-2022-35877**	N/A	O-GOA-IOTA-071122/4960
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	8.8	An OS command injection vulnerability exists in the web interface /action/iperf functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	N/A	O-GOA-IOTA-071122/4961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30603		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	8.8	An OS command injection vulnerability exists in the web interface /action/ipcamRecordPost functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-32586**	N/A	O-GOA-IOTA-071122/4962
Integer Overflow or Wraparound	25-Oct-2022	8.8	An integer overflow vulnerability exists in the web interface /action/ipcamRecordPost functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to memory corruption. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-32775**	N/A	O-GOA-IOTA-071122/4963
Use of Externally-Controlled Format String	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the UPnP logging functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and	N/A	O-GOA-IOTA-071122/4964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.9X. A specially-crafted UPnP negotiation can lead to memory corruption, information disclosure, and denial of service. An attacker can host a malicious UPnP service to trigger these vulnerabilities.This vulnerability arises from format string injection via `ST` and `Location` HTTP response headers, as used within the `DoEnumUPnPService` action handler. **CVE ID : CVE-2022-35878**		
Use of Externally-Controlled Format String	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the UPnP logging functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted UPnP negotiation can lead to memory corruption, information disclosure, and denial of service. An attacker can host a malicious UPnP service to trigger these vulnerabilities.This vulnerability arises from format string injection via `controlURL` XML tag, as used within the `DoUpdateUPnPbyService` action handler. **CVE ID : CVE-2022-35879**	N/A	O-GOA-IOTA-071122/4965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the UPnP logging functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted UPnP negotiation can lead to memory corruption, information disclosure, and denial of service. An attacker can host a malicious UPnP service to trigger these vulnerabilities.This vulnerability arises from format string injection via `NewInternalClient` XML tag, as used within the `DoUpdateUPnPbyService` action handler. **CVE ID : CVE-2022-35880**	N/A	O-GOA-IOTA-071122/4966
Use of Externally-Controlled Format String	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the UPnP logging functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted UPnP negotiation can lead to memory corruption, information disclosure, and denial of service. An attacker can host a malicious UPnP service to trigger these vulnerabilities.This vulnerability arises from format string injection via `errorCode` and `errorDescription` XML	N/A	O-GOA-IOTA-071122/4967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tags, as used within the `DoUpdateUPnPbyService` action handler. **CVE ID : CVE-2022-35881**		
Use of Externally-Controlled Format String	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted HTTP request can lead to memory corruption, information disclosure and denial of service. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability arises from format string injection via the `ssid_hex` HTTP parameter, as used within the `/action/wirelessConnect` handler. **CVE ID : CVE-2022-35884**	N/A	O-GOA-IOTA-071122/4968
Use of Externally-Controlled Format String	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted HTTP request can lead to memory corruption, information disclosure and denial of service. An attacker can make an	N/A	O-GOA-IOTA-071122/4969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated HTTP request to trigger these vulnerabilities.This vulnerability arises from format string injection via the `wpapsk_hex` HTTP parameter, as used within the `/action/wirelessConnect` handler. **CVE ID : CVE-2022-35885**		
Use of Externally-Controlled Format String	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted HTTP request can lead to memory corruption, information disclosure and denial of service. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability arises from format string injection via the `default_key_id` and `key` HTTP parameters, as used within the `/action/wirelessConnect` handler. **CVE ID : CVE-2022-35886**	N/A	O-GOA-IOTA-071122/4970
Use of Externally-Controlle	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the web interface /action/wirelessConnect functionality of Abode	N/A	O-GOA-IOTA-071122/4971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Format String			Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted HTTP request can lead to memory corruption, information disclosure and denial of service. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability arises from format string injection via the `default_key_id` HTTP parameter, as used within the `/action/wirelessConnect` handler. **CVE ID : CVE-2022-35887**		
Authentication Bypass by Capture-replay	25-Oct-2022	8.1	An information disclosure vulnerability exists in the XFINDER functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted man-in-the-middle attack can lead to increased privileges. An attacker can perform a man-in-the-middle attack to trigger this vulnerability. **CVE ID : CVE-2022-29475**	N/A	O-GOA-IOTA-071122/4972
Active Debug Code	25-Oct-2022	7.5	A denial of service vulnerability exists in the XCMD doDebug functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to denial	N/A	O-GOA-IOTA-071122/4973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of service. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-32760**		
Double Free	25-Oct-2022	6.5	A double-free vulnerability exists in the web interface /action/ipcamSetParamPost functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to memory corruption. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-32574**	N/A	O-GOA-IOTA-071122/4974
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	10	Four OS command injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A XCMD can lead to arbitrary command execution. An attacker can send a sequence of malicious commands to trigger these vulnerabilities.This vulnerability specifically focuses on the unsafe use of the `WL_SSID` and `WL_SSID_HEX` configuration values in the function at offset	N/A	O-GOA-IOTA-071122/4975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`0x1c7d28` of firmware 6.9Z. **CVE ID : CVE-2022-33192**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	10	Four OS command injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A XCMD can lead to arbitrary command execution. An attacker can send a sequence of malicious commands to trigger these vulnerabilities.This vulnerability focuses on the unsafe use of the `WL_DefaultKeyID` in the function located at offset `0x1c7d28` of firmware 6.9Z, and even more specifically on the command execution occuring at offset `0x1c7fac`. **CVE ID : CVE-2022-33195**	N/A	O-GOA-IOTA-071122/4976
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	10	Four OS command injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A XCMD can lead to arbitrary command execution. An attacker can send a sequence of malicious commands to trigger these	N/A	O-GOA-IOTA-071122/4977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities.This vulnerability focuses on the unsafe use of the `WL_Key` and `WL_DefaultKeyID` configuration values in the function located at offset `0x1c7d28` of firmware 6.9Z , and even more specifically on the command execution occuring at offset `0x1c7f6c`. **CVE ID : CVE-2022-33194**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	10	Four OS command injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A XCMD can lead to arbitrary command execution. An attacker can send a sequence of malicious commands to trigger these vulnerabilities.This vulnerability specifically focuses on the unsafe use of the `WL_WPAPSK` configuration value in the function located at offset `0x1c7d28` of firmware 6.9Z. **CVE ID : CVE-2022-33193**	N/A	O-GOA-IOTA-071122/4978
Affected Version(s): 6.9z					
Improper Neutralization of	25-Oct-2022	9.9	Four OS command injection vulnerabilities exists in the web	N/A	O-GOA-IOTA-071122/4979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability focuses on the unsafe use of the `key` and `default_key_id` HTTP parameters to construct an OS Command crafted at offset `0x19b1f4` of the `/root/hpgw` binary included in firmware 6.9Z. **CVE ID : CVE-2022-33206**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.9	Four OS command injection vulnerabilities exists in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability focuses on the unsafe use of the	N/A	O-GOA-IOTA-071122/4980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`wpapsk_hex` HTTP parameter to construct an OS Command at offset `0x19b0ac` of the `/root/hpgw` binary included in firmware 6.9Z. **CVE ID : CVE-2022-33205**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.9	Four OS command injection vulnerabilities exists in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability focuses on a second unsafe use of the `default_key_id` HTTP parameter to construct an OS Command at offset `0x19B234` of the `/root/hpgw` binary included in firmware 6.9Z. **CVE ID : CVE-2022-33207**	N/A	O-GOA-IOTA-071122/4981
Improper Neutralization of Special Elements used in an OS	25-Oct-2022	9.9	Four OS command injection vulnerabilities exists in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-	N/A	O-GOA-IOTA-071122/4982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability focuses on the unsafe use of the `ssid_hex` HTTP parameter to construct an OS Command at offset `0x19afc0` of the `/root/hpgw` binary included in firmware 6.9Z. **CVE ID : CVE-2022-33204**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.8	An os command injection vulnerability exists in the web interface util_set_abode_code functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-27804**	N/A	O-GOA-IOTA-071122/4983
Improper Access Control	25-Oct-2022	9.8	An authentication bypass vulnerability exists in the GHOME control functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted	N/A	O-GOA-IOTA-071122/4984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network request can lead to arbitrary XCMD execution. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-27805**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.8	An OS command injection vulnerability exists in the web interface util_set_serial_mac functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-29472**	N/A	O-GOA-IOTA-071122/4985
Use of Externally-Controlled Format String	25-Oct-2022	9.8	A format string injection vulnerability exists in the XCMD getVarHA functionality of abode systems, inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to memory corruption, information disclosure, and denial of service. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-35244**	N/A	O-GOA-IOTA-071122/4986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	25-Oct-2022	9.8	An authentication bypass vulnerability exists in the web interface /action/factory* functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP header can lead to authentication bypass. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-29477**	N/A	O-GOA-IOTA-071122/4987
Active Debug Code	25-Oct-2022	9.8	An OS command injection vulnerability exists in the console_main_loop :sys functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z. A specially-crafted XCMD can lead to arbitrary command execution. An attacker can send an XML payload to trigger this vulnerability. **CVE ID : CVE-2022-29520**	N/A	O-GOA-IOTA-071122/4988
Use of Hard-coded Credentials	25-Oct-2022	9.8	A hard-coded password vulnerability exists in the telnet functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z. Use of a hard-coded root password can lead to arbitrary command execution. An attacker can authenticate with hard-coded credentials	N/A	O-GOA-IOTA-071122/4989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to trigger this vulnerability. **CVE ID : CVE-2022-29889**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.8	An OS command injection vulnerability exists in the XCMD setUPnP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to arbitrary command execution. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-30541**	N/A	O-GOA-IOTA-071122/4990
Stack-based Buffer Overflow	25-Oct-2022	9.8	A stack-based buffer overflow vulnerability exists in the XCMD setIPCam functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to remote code execution. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-32454**	N/A	O-GOA-IOTA-071122/4991
Use of Externally-Controlled Format String	25-Oct-2022	9.8	A format string injection vulnerability exists in the ghome_process_control_packet functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A	N/A	O-GOA-IOTA-071122/4992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially-crafted XCMD can lead to memory corruption, information disclosure and denial of service. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-33938**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.8	An OS command injection vulnerability exists in the XCMD doDebug functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to arbitrary command execution. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-32773**	N/A	O-GOA-IOTA-071122/4993
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.8	An OS command injection vulnerability exists in the XCMD setAlexa functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z. A specially-crafted XCMD can lead to arbitrary command execution. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-33189**	N/A	O-GOA-IOTA-071122/4994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	25-Oct-2022	9.8	Four format string injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. Specially-crafted configuration values can lead to memory corruption, information disclosure and denial of service. An attacker can modify a configuration value and then execute an XCMD to trigger these vulnerabilities.This vulnerability arises from format string injection via the `ssid` and `ssid_hex` configuration parameters, as used within the `testWifiAP` XCMD handler **CVE ID : CVE-2022-35874**	N/A	O-GOA-IOTA-071122/4995
Use of Externally-Controlled Format String	25-Oct-2022	9.8	Four format string injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. Specially-crafted configuration values can lead to memory corruption, information disclosure and denial of service. An attacker can modify a configuration value and then execute an XCMD to trigger these vulnerabilities.This	N/A	O-GOA-IOTA-071122/4996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability arises from format string injection via the `wpapsk` configuration parameter, as used within the `testWifiAP` XCMD handler **CVE ID : CVE-2022-35875**		
Use of Externally-Controlled Format String	25-Oct-2022	9.8	Four format string injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. Specially-crafted configuration values can lead to memory corruption, information disclosure and denial of service. An attacker can modify a configuration value and then execute an XCMD to trigger these vulnerabilities.This vulnerability arises from format string injection via the `default_key_id` and `key` configuration parameters, as used within the `testWifiAP` XCMD handler **CVE ID : CVE-2022-35876**	N/A	O-GOA-IOTA-071122/4997
Use of Externally-Controlled Format String	25-Oct-2022	9.8	Four format string injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. Specially-crafted	N/A	O-GOA-IOTA-071122/4998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration values can lead to memory corruption, information disclosure and denial of service. An attacker can modify a configuration value and then execute an XCMD to trigger these vulnerabilities.This vulnerability arises from format string injection via the `default_key_id` configuration parameter, as used within the `testWifiAP` XCMD handler **CVE ID : CVE-2022-35877**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	8.8	An OS command injection vulnerability exists in the web interface /action/iperf functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-30603**	N/A	O-GOA-IOTA-071122/4999
Improper Neutralization of Special Elements used in an OS Command	25-Oct-2022	8.8	An OS command injection vulnerability exists in the web interface /action/ipcamRecordPost functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and	N/A	O-GOA-IOTA-071122/5000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-32586**		
Integer Overflow or Wraparound	25-Oct-2022	8.8	An integer overflow vulnerability exists in the web interface /action/ipcamRecordPost functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to memory corruption. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-32775**	N/A	O-GOA-IOTA-071122/5001
Use of Externally-Controlled Format String	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted HTTP request can lead to memory corruption, information disclosure and denial of service. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability arises from	N/A	O-GOA-IOTA-071122/5002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			format string injection via the `default_key_id` HTTP parameter, as used within the `/action/wirelessConnect` handler. **CVE ID : CVE-2022-35887**		
Use of Externally-Controlled Format String	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the UPnP logging functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted UPnP negotiation can lead to memory corruption, information disclosure, and denial of service. An attacker can host a malicious UPnP service to trigger these vulnerabilities.This vulnerability arises from format string injection via `ST` and `Location` HTTP response headers, as used within the `DoEnumUPnPService` action handler. **CVE ID : CVE-2022-35878**	N/A	O-GOA-IOTA-071122/5003
Use of Externally-Controlled Format String	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the UPnP logging functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted UPnP negotiation can lead to memory corruption, information disclosure, and denial of	N/A	O-GOA-IOTA-071122/5004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service. An attacker can host a malicious UPnP service to trigger these vulnerabilities.This vulnerability arises from format string injection via `controlURL` XML tag, as used within the `DoUpdateUPnPbyService` action handler. **CVE ID : CVE-2022-35879**		
Use of Externally-Controlled Format String	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the UPnP logging functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted UPnP negotiation can lead to memory corruption, information disclosure, and denial of service. An attacker can host a malicious UPnP service to trigger these vulnerabilities.This vulnerability arises from format string injection via `NewInternalClient` XML tag, as used within the `DoUpdateUPnPbyService` action handler. **CVE ID : CVE-2022-35880**	N/A	O-GOA-IOTA-071122/5005
Use of Externally-Controlled Format String	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the UPnP logging functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted	N/A	O-GOA-IOTA-071122/5006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UPnP negotiation can lead to memory corruption, information disclosure, and denial of service. An attacker can host a malicious UPnP service to trigger these vulnerabilities.This vulnerability arises from format string injection via `errorCode` and `errorDescription` XML tags, as used within the `DoUpdateUPnPbyService` action handler. **CVE ID : CVE-2022-35881**		
Use of Externally-Controlled Format String	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted HTTP request can lead to memory corruption, information disclosure and denial of service. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability arises from format string injection via the `ssid_hex` HTTP parameter, as used within the `/action/wirelessConnect` handler. **CVE ID : CVE-2022-35884**	N/A	O-GOA-IOTA-071122/5007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted HTTP request can lead to memory corruption, information disclosure and denial of service. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability arises from format string injection via the `wpapsk_hex` HTTP parameter, as used within the `/action/wirelessConnect` handler. **CVE ID : CVE-2022-35885**	N/A	O-GOA-IOTA-071122/5008
Use of Externally-Controlled Format String	25-Oct-2022	8.8	Four format string injection vulnerabilities exist in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted HTTP request can lead to memory corruption, information disclosure and denial of service. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability arises from format string injection	N/A	O-GOA-IOTA-071122/5009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via the `default_key_id` and `key` HTTP parameters, as used within the `/action/wirelessConnect` handler. **CVE ID : CVE-2022-35886**		
Authentication Bypass by Capture-replay	25-Oct-2022	8.1	An information disclosure vulnerability exists in the XFINDER functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted man-in-the-middle attack can lead to increased privileges. An attacker can perform a man-in-the-middle attack to trigger this vulnerability. **CVE ID : CVE-2022-29475**	N/A	O-GOA-IOTA-071122/5010
Active Debug Code	25-Oct-2022	7.5	A denial of service vulnerability exists in the XCMD doDebug functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to denial of service. An attacker can send a malicious XML payload to trigger this vulnerability. **CVE ID : CVE-2022-32760**	N/A	O-GOA-IOTA-071122/5011
Double Free	25-Oct-2022	6.5	A double-free vulnerability exists in the web interface /action/ipcamSetParamPost functionality of	N/A	O-GOA-IOTA-071122/5012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to memory corruption. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-32574**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	10	Four OS command injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A XCMD can lead to arbitrary command execution. An attacker can send a sequence of malicious commands to trigger these vulnerabilities.This vulnerability focuses on the unsafe use of the `WL_Key` and `WL_DefaultKeyID` configuration values in the function located at offset `0x1c7d28` of firmware 6.9Z , and even more specifically on the command execution occuring at offset `0x1c7f6c`. **CVE ID : CVE-2022-33194**	N/A	O-GOA-IOTA-071122/5013
Improper Neutralization of	25-Oct-2022	10	Four OS command injection vulnerabilities exist in the XCMD	N/A	O-GOA-IOTA-071122/5014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A XCMD can lead to arbitrary command execution. An attacker can send a sequence of malicious commands to trigger these vulnerabilities.This vulnerability specifically focuses on the unsafe use of the `WL_WPAPSK` configuration value in the function located at offset `0x1c7d28` of firmware 6.9Z. **CVE ID : CVE-2022-33193**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	10	Four OS command injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A XCMD can lead to arbitrary command execution. An attacker can send a sequence of malicious commands to trigger these vulnerabilities.This vulnerability specifically focuses on the unsafe use of the `WL_SSID` and `WL_SSID_HEX` configuration values in the function at offset `0x1c7d28` of firmware 6.9Z.	N/A	O-GOA-IOTA-071122/5015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33192		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	10	Four OS command injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A XCMD can lead to arbitrary command execution. An attacker can send a sequence of malicious commands to trigger these vulnerabilities.This vulnerability focuses on the unsafe use of the `WL_DefaultKeyID` in the function located at offset `0x1c7d28` of firmware 6.9Z, and even more specifically on the command execution occuring at offset `0x1c7fac`. **CVE ID : CVE-2022-33195**	N/A	O-GOA-IOTA-071122/5016
Vendor: gxgroup					
Product: gpon_ont_titanium_2122a_firmware					
Affected Version(s): t2122-v1.26exl					
Improper Restriction of Excessive Authentication Attempts	17-Oct-2022	9.8	An issue in GX Group GPON ONT Titanium 2122A T2122-V1.26EXL allows attackers to escalate privileges via a brute force attack at the login page. **CVE ID : CVE-2022-40055**	N/A	O-GXG-GPON-071122/5017
Vendor: ip-com					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ew9_firmware					
Affected Version(s): 15.11.0.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Oct-2022	9.8	IP-COM EW9 V15.11.0.14(9732) was discovered to contain a command injection vulnerability in the formSetDebugCfg function. **CVE ID : CVE-2022-43367**	N/A	O-IP--EW9_-071122/5018
Exposure of Sensitive Information to an Unauthorized Actor	27-Oct-2022	7.5	IP-COM EW9 V15.11.0.14(9732) allows unauthenticated attackers to access sensitive information via the checkLoginUser, ate, telnet, version, setDebugCfg, and boot interfaces. **CVE ID : CVE-2022-43366**	N/A	O-IP--EW9_-071122/5019
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	27-Oct-2022	7.5	IP-COM EW9 V15.11.0.14(9732) was discovered to contain a buffer overflow in the formSetDebugCfg function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string. **CVE ID : CVE-2022-43365**	N/A	O-IP--EW9_-071122/5020
N/A	27-Oct-2022	7.5	An access control issue in the password reset page of IP-COM EW9 V15.11.0.14(9732) allows unauthenticated attackers to arbitrarily	N/A	O-IP--EW9_-071122/5021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			change the admin password. **CVE ID : CVE-2022-43364**		
Vendor: iptime					
Product: nas1dual_firmware					
Affected Version(s): * Up to (excluding) 1.4.86					
Cross-Site Request Forgery (CSRF)	17-Oct-2022	8.8	This vulnerability occurs in user accounts creation and deleteion related pages of IPTIME NAS products. The vulnerability could be exploited by a lack of validation when a POST request is made to this page. An attacker can use this vulnerability to or delete user accounts, or to escalate arbitrary user privileges. **CVE ID : CVE-2022-23771**	N/A	O-IPT-NAS1-071122/5022
Product: nas2dual_firmware					
Affected Version(s): * Up to (excluding) 1.4.86					
Cross-Site Request Forgery (CSRF)	17-Oct-2022	8.8	This vulnerability occurs in user accounts creation and deleteion related pages of IPTIME NAS products. The vulnerability could be exploited by a lack of validation when a POST request is made to this page. An attacker can use this vulnerability to or delete user accounts, or to escalate arbitrary user privileges.	N/A	O-IPT-NAS2-071122/5023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23771		
Product: nas4dual_firmware					
Affected Version(s): * Up to (excluding) 1.4.86					
Cross-Site Request Forgery (CSRF)	17-Oct-2022	8.8	This vulnerability occurs in user accounts creation and deleteion related pages of IPTIME NAS products. The vulnerability could be exploited by a lack of validation when a POST request is made to this page. An attacker can use this vulnerability to or delete user accounts, or to escalate arbitrary user privileges. **CVE ID : CVE-2022-23771**	N/A	O-IPT-NAS4-071122/5024
Vendor: Juniper					
Product: junos					
Affected Version(s): * Up to (excluding) 15.1					
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition.	https://kb.juniper.net/JSA69873	O-JUN-JUNO-071122/5025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more and reviewing for backpressured output; for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on	https://kb.juniper.net/JSA69906	O-JUN-JUNO-071122/5026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Affected Version(s): * Up to (excluding) 18.4					
Use After Free	18-Oct-2022	5.9	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause Denial of Service (DoS). When a BGP session flap happens, a Use After Free of a memory location that was assigned to another object can occur, which will lead to an rpd crash. This is a race condition that is outside of the attacker's control and cannot be deterministically exploited. Continued flapping of BGP sessions can create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 version 19.2R1 and later versions; 19.3	https://kb.juniper.net/JSA69879	O-JUN-JUNO-071122/5027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22208**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS, Junos OS Evolved allows a network-based unauthenticated attacker to cause a Denial of Service (DoS). When a BGP flow route with redirect IP extended community is received, and the reachability to the next-hop of the corresponding redirect IP is flapping, the rpd process might crash. Whether the crash	https://kb.juniper.net/JSA69902	O-JUN-JUNO-071122/5028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occurs depends on the timing of the internally processing of these two events and is outside the attackers control. Please note that this issue also affects Route-Reflectors unless 'routing-options flow firewall-install-disable' is configured. This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.4 versions prior to 19.4R3-S8; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22220**		
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding	https://kb.juniper.net/JSA69890	O-JUN-JUNO-071122/5029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged %PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Affected Version(s): * Up to (excluding) 19.1					
Deserialization of Untrusted Data	18-Oct-2022	9.8	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request, deserialization may occur which could lead to unauthorized local file access or the ability to execute arbitrary commands. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22241**		
Inclusion of Functionality from Untrusted Control Sphere	18-Oct-2022	8.8	A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By chaining this vulnerability with other unspecified vulnerabilities, and by	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			circumventing existing attack requirements, successful exploitation could lead to a complete system compromise. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22246**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid	https://kb.juniper.net/JSA69901	O-JUN-JUNO-071122/5032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
N/A	18-Oct-2022	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in the processing of a malformed OSPF TLV in Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause the periodic packet management daemon (PPMD) process to go into an infinite loop, which in turn can cause protocols and functions reliant on PPMD such as	https://kb.juniper.net/JSA69874	O-JUN-JUNO-071122/5033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OSPF neighbor reachability to be impacted, resulting in a sustained Denial of Service (DoS) condition. The DoS condition persists until the PPMD process is manually restarted. This issue affects: Juniper Networks Junos OS: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S3-EVO; 21.1 versions prior to 21.1R2-EVO. **CVE ID : CVE-2022-22224**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site Scripting (XSS) vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker to run malicious scripts reflected off of J-Web to the victim's browser in the context of their session within J-Web. This issue affects Juniper Networks Junos OS all	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2022-22242**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	5.3	An XPath Injection vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22244**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	4.3	An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to add an XPath command to the XPath stream, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22243**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2022	4.3	A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built into Junos OS. The attacker should not be able to execute the file due to validation checks built into Junos OS. Successful exploitation of this vulnerability could lead to loss of filesystem integrity. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22245**		
Affected Version(s): * Up to (excluding) 19.2					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
Affected Version(s): * Up to (excluding) 19.4					
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions	https://kb.juniper.net/JSA69900	O-JUN-JUNO-071122/5039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**		
Affected Version(s): 15.1					
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or be transit packets. On devices such as the	https://kb.juniper.net/JSA69873	O-JUN-JUNO-071122/5040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more and reviewing for backpressured output; for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and	https://kb.juniper.net/JSA69906	O-JUN-JUNO-071122/5041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
Affected Version(s): 17.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6;	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	O-JUN-JUNO-071122/5042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Affected Version(s): 17.2					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	O-JUN-JUNO-071122/5043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Affected Version(s): 17.2x75					
Allocation of Resources Without	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory	https://kb.juniper.net/JSA69876, https://ww	O-JUN-JUNO-071122/5044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions	w.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Affected Version(s): 17.3					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	O-JUN-JUNO-071122/5045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Affected Version(s): 17.4					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	O-JUN-JUNO-071122/5047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Affected Version(s): 17.4r2					
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Affected Version(s): 18.1					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	O-JUN-JUNO-071122/5050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 18.1x75					
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO;	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Affected Version(s): 18.2					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	O-JUN-JUNO-071122/5053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Affected Version(s): 18.2x75					
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Affected Version(s): 18.2x75-d10					
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Affected Version(s): 18.2x75-d30					
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Affected Version(s): 18.3					
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	O-JUN-JUNO-071122/5058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Affected Version(s): 18.4					
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when	https://kb.juniper.net/JSA69873	O-JUN-JUNO-071122/5060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more and reviewing for backpressured output; for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	O-JUN-JUNO-071122/5061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	18-Oct-2022	5.9	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause Denial of Service (DoS). When a BGP session flap happens, a Use After Free of a memory location that was assigned to another object can occur, which will lead to an rpd crash. This is a race condition that is outside of the attacker's control and cannot be deterministically exploited. Continued flapping of BGP sessions can create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 version 19.2R1 and later versions; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to	https://kb.juniper.net/JSA69879	O-JUN-JUNO-071122/5063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22208**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS, Junos OS Evolved allows a network-based unauthenticated attacker to cause a Denial of Service (DoS). When a BGP flow route with redirect IP extended community is received, and the reachability to the next-hop of the corresponding redirect IP is flapping, the rpd process might crash. Whether the crash occurs depends on the timing of the internally processing of these two events and is outside the attackers control. Please note that this issue also affects Route-Reflectors unless 'routing-options flow firewall-install-disable' is configured. This issue affects: Juniper	https://kb.juniper.net/JSA69902	O-JUN-JUNO-071122/5064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.4 versions prior to 19.4R3-S8; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22220**		
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs	https://kb.juniper.net/JSA69890	O-JUN-JUNO-071122/5065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged %PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Affected Version(s): 19.1					
Deserialization of Untrusted Data	18-Oct-2022	9.8	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST request, deserialization may occur which could lead to unauthorized local file access or the ability to execute arbitrary commands. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22241**		
Inclusion of Functionality from Untrusted Control Sphere	18-Oct-2022	8.8	A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By chaining this vulnerability with other unspecified vulnerabilities, and by circumventing existing attack requirements, successful exploitation could lead to a complete system compromise. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22246**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2	https://kb.juniper.net/JSA69901	O-JUN-JUNO-071122/5068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or	https://kb.juniper.net/JSA69873	O-JUN-JUNO-071122/5069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more and reviewing for backpressured output; for example: GOT: 0x220702a8		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		
N/A	18-Oct-2022	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in the processing of a malformed OSPF TLV in Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause the periodic packet management daemon (PPMD) process to go into an infinite loop, which in turn can cause protocols and functions	https://kb.juniper.net/JSA69874	O-JUN-JUNO-071122/5070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reliant on PPMD such as OSPF neighbor reachability to be impacted, resulting in a sustained Denial of Service (DoS) condition. The DoS condition persists until the PPMD process is manually restarted. This issue affects: Juniper Networks Junos OS: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S3-EVO; 21.1 versions prior to 21.1R2-EVO. **CVE ID : CVE-2022-22224**		
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/stateme	O-JUN-JUNO-071122/5071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions	nt/vxlan.html#id-vxlan__d281e31	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue	https://kb.juniper.net/JSA69906	O-JUN-JUNO-071122/5072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Improper Neutralization of Input During Web Page Generatio	18-Oct-2022	6.1	A Cross-site Scripting (XSS) vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker to run malicious scripts	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n ('Cross-site Scripting')			reflected off of J-Web to the victim's browser in the context of their session within J-Web. This issue affects Juniper Networks Junos OS all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2022-22242**		
Use After Free	18-Oct-2022	5.9	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause Denial of Service (DoS). When a BGP session flap happens, a Use After Free of a memory location that was assigned to another object can occur, which will lead to an rpd crash. This is a race condition	https://kb.juniper.net/JSA69879	O-JUN-JUNO-071122/5075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that is outside of the attacker's control and cannot be deterministically exploited. Continued flapping of BGP sessions can create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 version 19.2R1 and later versions; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22208**		
Time-of-check Time-of-use	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Routing Protocol	https://kb.juniper.net/JSA69902	O-JUN-JUNO-071122/5076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			Daemon (rpd) of Juniper Networks Junos OS, Junos OS Evolved allows a network-based unauthenticated attacker to cause a Denial of Service (DoS). When a BGP flow route with redirect IP extended community is received, and the reachability to the next-hop of the corresponding redirect IP is flapping, the rpd process might crash. Whether the crash occurs depends on the timing of the internally processing of these two events and is outside the attackers control. Please note that this issue also affects Route-Reflectors unless 'routing-options flow firewall-install-disable' is configured. This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.4 versions prior to 19.4R3-S8; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to 21.1R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22220**		
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause.	https://kb.juniper.net/JSA69890	O-JUN-JUNO-071122/5077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged %PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	5.3	An XPath Injection vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22244**	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
XML Injection (aka Blind XPath Injection)	18-Oct-2022	4.3	An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to add an XPath command to the XPath stream, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22243**	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5079
Improper Limitation of a Pathname	18-Oct-2022	4.3	A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built into Junos OS. The attacker should not be able to execute the file due to validation checks built into Junos OS. Successful exploitation of this vulnerability could lead to loss of filesystem integrity. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22245**		
Affected Version(s): 19.2					
Deserialization of Untrusted Data	18-Oct-2022	9.8	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST request, deserialization may occur which could lead to unauthorized local file access or the ability to execute arbitrary commands. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22241**		
Inclusion of Functionality from Untrusted Control Sphere	18-Oct-2022	8.8	A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			chaining this vulnerability with other unspecified vulnerabilities, and by circumventing existing attack requirements, successful exploitation could lead to a complete system compromise. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22246**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker	https://kb.juniper.net/JSA69901	O-JUN-JUNO-071122/5083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending	https://kb.juniper.net/JSA69873	O-JUN-JUNO-071122/5084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more and reviewing for backpressured output; for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in the processing of a malformed OSPF TLV in Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause the periodic packet management daemon (PPMD) process to go into an infinite loop, which in turn can cause protocols and functions reliant on PPMD such as OSPF neighbor reachability to be impacted, resulting in a sustained Denial of Service (DoS) condition. The DoS condition persists until the PPMD process is manually restarted. This issue affects: Juniper Networks Junos OS: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S3-EVO;	https://kb.juniper.net/JSA69874	O-JUN-JUNO-071122/5085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.1 versions prior to 21.1R2-EVO. **CVE ID : CVE-2022-22224**		
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	O-JUN-JUNO-071122/5086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Check for Unusual or Exceptional	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conditions			Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions	https://kb.juniper.net/JSA69906	O-JUN-JUNO-071122/5089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site Scripting (XSS) vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker to run malicious scripts reflected off of J-Web to the victim's browser in the context of their session within J-Web. This issue affects Juniper Networks Junos OS all versions prior to 19.1R3-	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2022-22242**		
Use After Free	18-Oct-2022	5.9	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause Denial of Service (DoS). When a BGP session flap happens, a Use After Free of a memory location that was assigned to another object can occur, which will lead to an rpd crash. This is a race condition that is outside of the attacker's control and cannot be deterministically exploited. Continued flapping of BGP sessions can create a sustained	https://kb.juniper.net/JSA69879	O-JUN-JUNO-071122/5092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 version 19.2R1 and later versions; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22208**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated attacker with an established BGP session to cause a Denial of	https://kb.juniper.net/JSA69875	O-JUN-JUNO-071122/5093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS). In a BGP multipath scenario, when one of the contributing routes is flapping often and rapidly, rpd may crash. As this crash depends on whether a route is a contributing route, and on the internal timing of the events triggered by the flap this vulnerability is outside the direct control of a potential attacker. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R2-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions 19.2 versions prior to 19.2R2, 19.3R1 and above prior to 20.2R1. Juniper Networks Junos OS Evolved versions prior to 20.2R1-EVO.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22225		
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0	https://kb.juniper.net/JSA69890	O-JUN-JUNO-071122/5094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sfp-0/1/2 SFP unplugged %PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
XML Injection (aka Blind XPath Injection)	18-Oct-2022	5.3	An XPath Injection vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22244**	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5095
XML Injection (aka Blind XPath Injection)	18-Oct-2022	4.3	An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper Networks Junos OS allows an authenticated	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to add an XPath command to the XPath stream, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22243**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2022	4.3	A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built into Junos OS. The attacker should not be	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to execute the file due to validation checks built into Junos OS. Successful exploitation of this vulnerability could lead to loss of filesystem integrity. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22245**		
Affected Version(s): 19.3					
Deserialization of Untrusted Data	18-Oct-2022	9.8	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST request, deserialization may occur which could lead to unauthorized	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local file access or the ability to execute arbitrary commands. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22241**		
Inclusion of Functionality from Untrusted Control Sphere	18-Oct-2022	8.8	A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By chaining this vulnerability with other unspecified vulnerabilities, and by circumventing existing attack requirements, successful exploitation	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to a complete system compromise. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22246**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate	https://kb.juniper.net/JSA69901	O-JUN-JUNO-071122/5100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these	https://kb.juniper.net/JSA69873	O-JUN-JUNO-071122/5101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more and reviewing for backpressured output; for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		
N/A	18-Oct-2022	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in the processing of a malformed OSPF TLV in Juniper Networks Junos OS and Junos OS Evolved allows an	https://kb.juniper.net/JSA69874	O-JUN-JUNO-071122/5102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated adjacent attacker to cause the periodic packet management daemon (PPMD) process to go into an infinite loop, which in turn can cause protocols and functions reliant on PPMD such as OSPF neighbor reachability to be impacted, resulting in a sustained Denial of Service (DoS) condition. The DoS condition persists until the PPMD process is manually restarted. This issue affects: Juniper Networks Junos OS: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S3-EVO; 21.1 versions prior to 21.1R2-EVO. **CVE ID : CVE-2022-22224**		
Allocation of Resources Without	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory	https://kb.juniper.net/JSA69876, https://ww	O-JUN-JUNO-071122/5103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions	w.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial	https://kb.juniper.net/JSA69906	O-JUN-JUNO-071122/5106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site Scripting (XSS) vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker to run malicious scripts reflected off of J-Web to the victim's browser in the context of their session within J-Web. This issue affects Juniper Networks Junos OS all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2022-22242**		
Use After Free	18-Oct-2022	5.9	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause Denial of Service (DoS). When a BGP session flap happens, a Use After Free of a memory location that was assigned to another object can occur, which will lead to an rpd crash. This is a race condition that is outside of the attacker's control and cannot be deterministically exploited. Continued flapping of BGP sessions can create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 version 19.2R1 and later versions; 19.3	https://kb.juniper.net/JSA69879	O-JUN-JUNO-071122/5109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22208**		
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected	https://kb.juniper.net/JSA69890	O-JUN-JUNO-071122/5110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged %PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	5.3	An XPath Injection vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22244**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	4.3	An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to add an XPath command to the XPath stream, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22243**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2022	4.3	A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built into Junos OS. The attacker should not be able to execute the file due to validation checks built into Junos OS. Successful exploitation of this vulnerability could lead to loss of filesystem integrity. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22245**		
Affected Version(s): 19.4					
Deserialization of Untrusted Data	18-Oct-2022	9.8	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST request, deserialization may occur which could lead to unauthorized local file access or the ability to execute arbitrary commands. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2,	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22241**		
Inclusion of Functionality from Untrusted Control Sphere	18-Oct-2022	8.8	A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By chaining this vulnerability with other unspecified vulnerabilities, and by circumventing existing attack requirements, successful exploitation could lead to a complete system compromise. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22246**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2.	https://kb.juniper.net/JSA69900	O-JUN-JUNO-071122/5116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22201		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**	https://kb.juniper.net/JSA69901	O-JUN-JUNO-071122/5117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-	https://kb.juniper.net/JSA69873	O-JUN-JUNO-071122/5118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more and reviewing for backpressured output; for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		
N/A	18-Oct-2022	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in the processing of a malformed OSPF TLV in Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause the periodic packet management daemon (PPMD) process to go into an infinite loop, which in turn can cause protocols and functions reliant on PPMD such as OSPF neighbor reachability to be impacted, resulting in a sustained Denial of Service (DoS) condition. The DoS condition persists until the PPMD process is manually restarted. This issue affects: Juniper Networks Junos OS: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S3; 19.4 versions	https://kb.juniper.net/JSA69874	O-JUN-JUNO-071122/5119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.4R3-S9; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S3-EVO; 21.1 versions prior to 21.1R2-EVO. **CVE ID : CVE-2022-22224**		
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	O-JUN-JUNO-071122/5120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors	https://kb.juniper.net/JSA69906	O-JUN-JUNO-071122/5123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Improper Neutralization of	18-Oct-2022	6.1	A Cross-site Scripting (XSS) vulnerability in the J-Web component of	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Juniper Networks Junos OS allows an unauthenticated attacker to run malicious scripts reflected off of J-Web to the victim's browser in the context of their session within J-Web. This issue affects Juniper Networks Junos OS all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2022-22242**		
Use After Free	18-Oct-2022	5.9	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause Denial of Service (DoS). When a BGP session flap happens, a Use After Free of a memory location that	https://kb.juniper.net/JSA69879	O-JUN-JUNO-071122/5126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was assigned to another object can occur, which will lead to an rpd crash. This is a race condition that is outside of the attacker's control and cannot be deterministically exploited. Continued flapping of BGP sessions can create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 version 19.2R1 and later versions; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22208**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS, Junos OS Evolved allows a network-based unauthenticated attacker to cause a Denial of Service (DoS). When a BGP flow route with redirect IP extended community is received, and the reachability to the next-hop of the corresponding redirect IP is flapping, the rpd process might crash. Whether the crash occurs depends on the timing of the internally processing of these two events and is outside the attackers control. Please note that this issue also affects Route-Reflectors unless 'routing-options flow firewall-install-disable' is configured. This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.4 versions prior to 19.4R3-S8; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper	https://kb.juniper.net/JSA69902	O-JUN-JUNO-071122/5127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22220**		
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and	https://kb.juniper.net/JSA69890	O-JUN-JUNO-071122/5128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged %PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Missing Release of Memory after Effective Lifetime	18-Oct-2022	5.5	An Allocation of Resources Without Limits or Throttling and a Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated low privileged attacker to cause a Denial of Sevice (DoS). In a high-scaled BGP routing environment with rib-sharding enabled, two issues may occur when executing a specific CLI command. One is a memory leak issue with rpd where the leak rate is not constant, and the other is a temporary spike in rpd memory usage during command execution. This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1	https://kb.juniper.net/JSA69896	O-JUN-JUNO-071122/5129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R1-S2-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. **CVE ID : CVE-2022-22240**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	5.3	An XPath Injection vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22244**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	4.3	An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to add an XPath command to the XPath stream, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22243**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2022	4.3	A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built into Junos OS. The attacker should not be able to execute the file due to validation checks built into Junos OS. Successful exploitation of this vulnerability could lead to loss of filesystem integrity. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22245**		
Affected Version(s): 20.1					
Deserialization of Untrusted Data	18-Oct-2022	9.8	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST request, deserialization may occur which could lead to unauthorized local file access or the ability to execute arbitrary commands. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2,	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22241**		
Inclusion of Functionality from Untrusted Control Sphere	18-Oct-2022	8.8	A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By chaining this vulnerability with other unspecified vulnerabilities, and by circumventing existing attack requirements, successful exploitation could lead to a complete system compromise. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22246**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2.	https://kb.juniper.net/JSA69900	O-JUN-JUNO-071122/5135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22201		
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-	https://kb.juniper.net/JSA69873	O-JUN-JUNO-071122/5136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more and reviewing for backpressured output; for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		
N/A	18-Oct-2022	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in the processing of a malformed OSPF TLV in Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause the periodic packet management daemon (PPMD) process to go into an infinite loop, which in turn can cause protocols and functions reliant on PPMD such as OSPF neighbor reachability to be impacted, resulting in a sustained Denial of Service (DoS) condition. The DoS condition persists until the PPMD process is manually restarted. This issue affects: Juniper Networks Junos OS: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-	https://kb.juniper.net/JSA69874	O-JUN-JUNO-071122/5137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S5; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S3-EVO; 21.1 versions prior to 21.1R2-EVO. **CVE ID : CVE-2022-22224**		
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	O-JUN-JUNO-071122/5138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error.	https://kb.juniper.net/JSA69906	O-JUN-JUNO-071122/5141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071): EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site Scripting (XSS) vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker to run malicious scripts reflected off of J-Web to the victim's browser in the context of their session within J-Web. This issue affects Juniper Networks Junos OS all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2022-22242**	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5143
Use After Free	18-Oct-2022	5.9	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause Denial of Service (DoS). When a BGP	https://kb.juniper.net/JSA69879	O-JUN-JUNO-071122/5144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session flap happens, a Use After Free of a memory location that was assigned to another object can occur, which will lead to an rpd crash. This is a race condition that is outside of the attacker's control and cannot be deterministically exploited. Continued flapping of BGP sessions can create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 version 19.2R1 and later versions; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22208		
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0	https://kb.juniper.net/JSA69890	O-JUN-JUNO-071122/5145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sfp-0/1/2 SFP unplugged %PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
XML Injection (aka Blind XPath Injection)	18-Oct-2022	5.3	An XPath Injection vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22244**	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5146
XML Injection (aka Blind XPath Injection)	18-Oct-2022	4.3	An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper Networks Junos OS allows an authenticated	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to add an XPath command to the XPath stream, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22243**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2022	4.3	A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built into Junos OS. The attacker should not be	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to execute the file due to validation checks built into Junos OS. Successful exploitation of this vulnerability could lead to loss of filesystem integrity. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22245**		
Affected Version(s): 20.2					
Deserialization of Untrusted Data	18-Oct-2022	9.8	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST request, deserialization may occur which could lead to unauthorized	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local file access or the ability to execute arbitrary commands. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22241**		
Inclusion of Functionality from Untrusted Control Sphere	18-Oct-2022	8.8	A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By chaining this vulnerability with other unspecified vulnerabilities, and by circumventing existing attack requirements, successful exploitation	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to a complete system compromise. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22246**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a	https://kb.juniper.net/JSA69900	O-JUN-JUNO-071122/5151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to	https://kb.juniper.net/JSA69901	O-JUN-JUNO-071122/5152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and	https://kb.juniper.net/JSA69873	O-JUN-JUNO-071122/5153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 |		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			refresh 1 | no-more and reviewing for backpressured output; for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will	https://kb.juniper.net/JSA69891	O-JUN-JUNO-071122/5154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
N/A	18-Oct-2022	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in the processing of a malformed OSPF TLV in Juniper Networks Junos	https://kb.juniper.net/JSA69874	O-JUN-JUNO-071122/5155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause the periodic packet management daemon (PPMD) process to go into an infinite loop, which in turn can cause protocols and functions reliant on PPMD such as OSPF neighbor reachability to be impacted, resulting in a sustained Denial of Service (DoS) condition. The DoS condition persists until the PPMD process is manually restarted. This issue affects: Juniper Networks Junos OS: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S3-EVO; 21.1 versions prior to 21.1R2-EVO. **CVE ID : CVE-2022-22224**		
Allocation of	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600,	https://kb.juniper.net/JS	O-JUN-JUNO-071122/5156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resources Without Limits or Throttling			QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions	A69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an	https://kb.juniper.net/JSA69906	O-JUN-JUNO-071122/5159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(429 8): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site Scripting (XSS) vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker to run malicious scripts reflected off of J-Web to the victim's browser in the context of their session within J-Web. This issue affects Juniper Networks Junos OS all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2022-22242**		
Use After Free	18-Oct-2022	5.9	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause Denial of Service (DoS). When a BGP session flap happens, a Use After Free of a memory location that was assigned to another object can occur, which will lead to an rpd crash. This is a race condition that is outside of the attacker's control and cannot be deterministically exploited. Continued flapping of BGP sessions can create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-	https://kb.juniper.net/JSA69879	O-JUN-JUNO-071122/5162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S8; 19.2 version 19.2R1 and later versions; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22208**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS, Junos OS Evolved allows a network-based unauthenticated attacker to cause a Denial of Service (DoS). When a BGP flow route with redirect IP extended community is received, and the reachability to the next-hop of the corresponding redirect IP is flapping, the rpd	https://kb.juniper.net/JSA69902	O-JUN-JUNO-071122/5163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process might crash. Whether the crash occurs depends on the timing of the internally processing of these two events and is outside the attackers control. Please note that this issue also affects Route-Reflectors unless 'routing-options flow firewall-install-disable' is configured. This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.4 versions prior to 19.4R3-S8; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22220**		
Time-of-check Time-of-use (TOCTOU	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and	https://kb.juniper.net/JSA69875	O-JUN-JUNO-071122/5164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
) Race Condition			Junos OS Evolved allows an unauthenticated attacker with an established BGP session to cause a Denial of Service (DoS). In a BGP multipath scenario, when one of the contributing routes is flapping often and rapidly, rpd may crash. As this crash depends on whether a route is a contributing route, and on the internal timing of the events triggered by the flap this vulnerability is outside the direct control of a potential attacker. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R2-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions 19.2 versions prior to 19.2R2, 19.3R1 and above prior		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to 20.2R1. Juniper Networks Junos OS Evolved versions prior to 20.2R1-EVO. **CVE ID : CVE-2022-22225**		
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by	https://kb.juniper.net/JSA69890	O-JUN-JUNO-071122/5165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged %PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Missing Release of Memory after Effective Lifetime	18-Oct-2022	5.5	An Allocation of Resources Without Limits or Throttling and a Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated low privileged attacker to cause a Denial of Sevice (DoS). In a high-scaled BGP routing environment with rib-sharding enabled, two issues may occur when executing a specific CLI command. One is a memory leak issue with rpd where the leak rate is not constant, and the other is a temporary spike in rpd memory usage during command execution. This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R2. Juniper	https://kb.juniper.net/JSA69896	O-JUN-JUNO-071122/5166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS Evolved All versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R1-S2-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. **CVE ID : CVE-2022-22240**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	5.3	An XPath Injection vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22244**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	4.3	An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to add an XPath command to the XPath stream, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2,	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22243**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2022	4.3	A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built into Junos OS. The attacker should not be able to execute the file due to validation checks built into Junos OS. Successful exploitation of this vulnerability could lead to loss of filesystem integrity. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22245**		
Affected Version(s): 20.3					
Deserialization of Untrusted Data	18-Oct-2022	9.8	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST request, deserialization may occur which could lead to unauthorized local file access or the ability to execute arbitrary commands. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2.	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22241		
Inclusion of Functionality from Untrusted Control Sphere	18-Oct-2022	8.8	A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By chaining this vulnerability with other unspecified vulnerabilities, and by circumventing existing attack requirements, successful exploitation could lead to a complete system compromise. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2.	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22246		
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**	https://kb.juniper.net/JSA69900	O-JUN-JUNO-071122/5172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**	https://kb.juniper.net/JSA69901	O-JUN-JUNO-071122/5173
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when	https://kb.juniper.net/JSA69873	O-JUN-JUNO-071122/5174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more and reviewing for backpressured output; for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions	https://kb.juniper.net/JSA69891	O-JUN-JUNO-071122/5175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
N/A	18-Oct-2022	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in the processing of a malformed OSPF TLV in Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause the periodic packet management daemon (PPMD) process to go into an infinite loop, which in turn can cause protocols and functions reliant on PPMD such as OSPF neighbor reachability to be impacted, resulting in a sustained Denial of Service (DoS) condition. The DoS condition persists until the PPMD process is manually restarted. This issue affects: Juniper Networks Junos OS: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-	https://kb.juniper.net/JSA69874	O-JUN-JUNO-071122/5176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S5; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S3-EVO; 21.1 versions prior to 21.1R2-EVO. **CVE ID : CVE-2022-22224**		
Allocation of Resources Without Limits or Throttling	18-Oct-2022	6.5	In VxLAN scenarios on EX4300-MP, EX4600, QFX5000 Series devices an Uncontrolled Memory Allocation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated adjacently located attacker sending specific packets to cause a Denial of Service (DoS) condition by crashing one or more PFE's when they are received and processed by the device. Upon automatic restart of the PFE, continued processing of these packets will cause the memory leak to reappear. Depending on the volume of packets received the attacker	https://kb.juniper.net/JSA69876, https://www.juniper.net/documentation/us/en/software/junos/ovsdb-vxlan/evpn-vxlan/topics/ref/statement/vxlan.html#id-vxlan__d281e31	O-JUN-JUNO-071122/5177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be able to create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP, EX4600, QFX5000 Series: 17.1 version 17.1R1 and later versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S7, 19.2R3-S1; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS versions prior to 17.1R1. **CVE ID : CVE-2022-22226**		
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error.	https://kb.juniper.net/JSA69906	O-JUN-JUNO-071122/5180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071): EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site Scripting (XSS) vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker to run malicious scripts reflected off of J-Web to the victim's browser in the context of their session within J-Web. This issue affects Juniper Networks Junos OS all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2022-22242**	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5182
Use After Free	18-Oct-2022	5.9	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause Denial of Service (DoS). When a BGP	https://kb.juniper.net/JSA69879	O-JUN-JUNO-071122/5183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session flap happens, a Use After Free of a memory location that was assigned to another object can occur, which will lead to an rpd crash. This is a race condition that is outside of the attacker's control and cannot be deterministically exploited. Continued flapping of BGP sessions can create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 version 19.2R1 and later versions; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22208		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS, Junos OS Evolved allows a network-based unauthenticated attacker to cause a Denial of Service (DoS). When a BGP flow route with redirect IP extended community is received, and the reachability to the next-hop of the corresponding redirect IP is flapping, the rpd process might crash. Whether the crash occurs depends on the timing of the internally processing of these two events and is outside the attackers control. Please note that this issue also affects Route-Reflectors unless 'routing-options flow firewall-install-disable' is configured. This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.4 versions prior to 19.4R3-S8; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to	https://kb.juniper.net/JSA69902	O-JUN-JUNO-071122/5184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22220**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated attacker with an established BGP session to cause a Denial of Service (DoS). In a BGP multipath scenario, when one of the contributing routes is flapping often and rapidly, rpd may crash. As this crash depends on whether a route is a contributing route, and on the internal timing of the events triggered by the flap this vulnerability is outside the direct control of a potential attacker. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 20.2 versions prior to 20.2R3-S4; 20.3 versions	https://kb.juniper.net/JSA69875	O-JUN-JUNO-071122/5185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R2-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions 19.2 versions prior to 19.2R2, 19.3R1 and above prior to 20.2R1. Juniper Networks Junos OS Evolved versions prior to 20.2R1-EVO. **CVE ID : CVE-2022-22225**		
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series	https://kb.juniper.net/JSA69890	O-JUN-JUNO-071122/5186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged %PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Missing Release of Memory after Effective Lifetime	18-Oct-2022	5.5	An Allocation of Resources Without Limits or Throttling and a Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated low privileged attacker to cause a Denial of Sevice (DoS). In a high-scaled BGP routing environment with rib-sharding enabled, two issues may occur when executing a specific CLI	https://kb.juniper.net/JSA69896	O-JUN-JUNO-071122/5187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command. One is a memory leak issue with rpd where the leak rate is not constant, and the other is a temporary spike in rpd memory usage during command execution. This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R1-S2-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. **CVE ID : CVE-2022-22240**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	5.3	An XPath Injection vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22244**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	4.3	An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to add an XPath command to the XPath stream, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22243**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2022	4.3	A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built into Junos OS. The attacker should not be able to execute the file due to validation checks built into Junos OS. Successful exploitation of this vulnerability could lead to loss of filesystem integrity. This issue	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22245**		
Affected Version(s): 20.4					
Deserialization of Untrusted Data	18-Oct-2022	9.8	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST request, deserialization may occur which could lead to unauthorized local file access or the ability to execute arbitrary commands. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22241**		
Inclusion of Functionality from Untrusted Control Sphere	18-Oct-2022	8.8	A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By chaining this vulnerability with other unspecified vulnerabilities, and by circumventing existing attack requirements, successful exploitation could lead to a complete system compromise. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22246**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with	https://kb.juniper.net/JSA69900	O-JUN-JUNO-071122/5193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to	https://kb.juniper.net/JSA69901	O-JUN-JUNO-071122/5194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or be transit packets. On devices such as the	https://kb.juniper.net/JSA69873	O-JUN-JUNO-071122/5195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more and reviewing for backpressured output; for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services	https://kb.juniper.net/JSA69891	O-JUN-JUNO-071122/5196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets	https://kb.juniper.net/JSA69892	O-JUN-JUNO-071122/5197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
N/A	18-Oct-2022	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in the processing of a malformed OSPF TLV in Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause the periodic packet management daemon (PPMD) process to go into an infinite loop, which in turn can cause protocols and functions reliant on PPMD such as OSPF neighbor reachability to be impacted, resulting in a sustained Denial of Service (DoS) condition.	https://kb.juniper.net/JSA69874	O-JUN-JUNO-071122/5198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The DoS condition persists until the PPMD process is manually restarted. This issue affects: Juniper Networks Junos OS: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S3-EVO; 21.1 versions prior to 21.1R2-EVO. **CVE ID : CVE-2022-22224**		
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Check for Unusual or	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22238		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-	https://kb.juniper.net/JSA69906	O-JUN-JUNO-071122/5201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site Scripting (XSS) vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker to run malicious scripts reflected off of J-Web to the victim's browser in the context of their session within J-Web. This issue affects Juniper	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2022-22242**		
Use After Free	18-Oct-2022	5.9	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause Denial of Service (DoS). When a BGP session flap happens, a Use After Free of a memory location that was assigned to another object can occur, which will lead to an rpd crash. This is a race condition that is outside of the attacker's control and cannot be deterministically exploited. Continued	https://kb.juniper.net/JSA69879	O-JUN-JUNO-071122/5204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flapping of BGP sessions can create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 version 19.2R1 and later versions; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22208**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS, Junos OS Evolved allows a network-based unauthenticated attacker	https://kb.juniper.net/JSA69902	O-JUN-JUNO-071122/5205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause a Denial of Service (DoS). When a BGP flow route with redirect IP extended community is received, and the reachability to the next-hop of the corresponding redirect IP is flapping, the rpd process might crash. Whether the crash occurs depends on the timing of the internally processing of these two events and is outside the attackers control. Please note that this issue also affects Route-Reflectors unless 'routing-options flow firewall-install-disable' is configured. This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.4 versions prior to 19.4R3-S8; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22220		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated attacker with an established BGP session to cause a Denial of Service (DoS). In a BGP multipath scenario, when one of the contributing routes is flapping often and rapidly, rpd may crash. As this crash depends on whether a route is a contributing route, and on the internal timing of the events triggered by the flap this vulnerability is outside the direct control of a potential attacker. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO	https://kb.juniper.net/JSA69875	O-JUN-JUNO-071122/5206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.2R2-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions 19.2 versions prior to 19.2R2, 19.3R1 and above prior to 20.2R1. Juniper Networks Junos OS Evolved versions prior to 20.2R1-EVO. **CVE ID : CVE-2022-22225**		
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of	https://kb.juniper.net/JSA69890	O-JUN-JUNO-071122/5207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged %PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Missing Release of Memory after Effective Lifetime	18-Oct-2022	5.5	An Allocation of Resources Without Limits or Throttling and a Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated low privileged attacker to cause a Denial of Sevice (DoS). In a high-scaled BGP routing environment with rib-sharding enabled, two issues may occur when executing a specific CLI command. One is a memory leak issue with rpd where the leak rate is not constant, and the other is a temporary spike in rpd memory usage during command execution. This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-	https://kb.juniper.net/JSA69896	O-JUN-JUNO-071122/5208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S5; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R1-S2-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. **CVE ID : CVE-2022-22240**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	5.3	An XPath Injection vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22244**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	4.3	An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to add an XPath command to the XPath stream, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22243**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2022	4.3	A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built into Junos OS. The attacker should not be able to execute the file due to validation checks built into Junos OS. Successful exploitation of this vulnerability could lead to loss of filesystem integrity. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22245**		
Affected Version(s): 21.1					
Deserialization of Untrusted Data	18-Oct-2022	9.8	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST request, deserialization may occur which could lead to unauthorized local file access or the ability to execute arbitrary commands. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22241**		
Inclusion of Functionality from Untrusted Control Sphere	18-Oct-2022	8.8	A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By chaining this vulnerability with other unspecified vulnerabilities, and by circumventing existing attack requirements, successful exploitation could lead to a complete system compromise. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22246**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions	https://kb.juniper.net/JSA69900	O-JUN-JUNO-071122/5214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2.	https://kb.juniper.net/JSA69901	O-JUN-JUNO-071122/5215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22218		
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-	https://kb.juniper.net/JSA69873	O-JUN-JUNO-071122/5216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more and reviewing for backpressured output; for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Type of Input vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS allows an attacker to cause an RPD memory leak leading to a Denial of Service (DoS). This memory leak only occurs when the attacker's packets are destined to any configured IPv6 address on the device. This issue affects: Juniper Networks Junos OS 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. **CVE ID : CVE-2022-22228**	https://kb.juniper.net/JSA69880	O-JUN-JUNO-071122/5217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper	https://kb.juniper.net/JSA69891	O-JUN-JUNO-071122/5218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**	https://kb.juniper.net/JSA69892	O-JUN-JUNO-071122/5219
N/A	18-Oct-2022	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in the processing of a malformed OSPF TLV in	https://kb.juniper.net/JSA69874	O-JUN-JUNO-071122/5220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause the periodic packet management daemon (PPMD) process to go into an infinite loop, which in turn can cause protocols and functions reliant on PPMD such as OSPF neighbor reachability to be impacted, resulting in a sustained Denial of Service (DoS) condition. The DoS condition persists until the PPMD process is manually restarted. This issue affects: Juniper Networks Junos OS: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S3-EVO; 21.1 versions prior to 21.1R2-EVO. **CVE ID : CVE-2022-22224**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0]	https://kb.juniper.net/JSA69906	O-JUN-JUNO-071122/5223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071): EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071): EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site Scripting (XSS) vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker to run malicious scripts reflected off of J-Web to the victim's browser in the context of their session within J-Web. This issue affects Juniper Networks Junos OS all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2022-22242**	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5225
Use After Free	18-Oct-2022	5.9	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and	https://kb.juniper.net/JSA69879	O-JUN-JUNO-071122/5226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS Evolved allows an unauthenticated network-based attacker to cause Denial of Service (DoS). When a BGP session flap happens, a Use After Free of a memory location that was assigned to another object can occur, which will lead to an rpd crash. This is a race condition that is outside of the attacker's control and cannot be deterministically exploited. Continued flapping of BGP sessions can create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 version 19.2R1 and later versions; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22208**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS, Junos OS Evolved allows a network-based unauthenticated attacker to cause a Denial of Service (DoS). When a BGP flow route with redirect IP extended community is received, and the reachability to the next-hop of the corresponding redirect IP is flapping, the rpd process might crash. Whether the crash occurs depends on the timing of the internally processing of these two events and is outside the attackers control. Please note that this issue also affects Route-Reflectors unless 'routing-options flow firewall-install-disable' is configured. This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to	https://kb.juniper.net/JSA69902	O-JUN-JUNO-071122/5227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.2R1-S8, 19.2R3-S4; 19.4 versions prior to 19.4R3-S8; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22220**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated attacker with an established BGP session to cause a Denial of Service (DoS). In a BGP multipath scenario, when one of the contributing routes is flapping often and rapidly, rpd may crash. As this crash depends on whether a route is a contributing route, and on the internal timing of the events triggered by the flap this vulnerability is outside the direct control of a	https://kb.juniper.net/JSA69875	O-JUN-JUNO-071122/5228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential attacker. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R2-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions 19.2 versions prior to 19.2R2, 19.3R1 and above prior to 20.2R1. Juniper Networks Junos OS Evolved versions prior to 20.2R1-EVO. **CVE ID : CVE-2022-22225**		
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally	https://kb.juniper.net/JSA69890	O-JUN-JUNO-071122/5229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged %PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Missing Release of Memory after Effective Lifetime	18-Oct-2022	5.5	An Allocation of Resources Without Limits or Throttling and a Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated low privileged attacker to cause a Denial of	https://kb.juniper.net/JSA69896	O-JUN-JUNO-071122/5230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sevice (DoS). In a high-scaled BGP routing environment with rib-sharding enabled, two issues may occur when executing a specific CLI command. One is a memory leak issue with rpd where the leak rate is not constant, and the other is a temporary spike in rpd memory usage during command execution. This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R1-S2-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. **CVE ID : CVE-2022-22240**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
XML Injection (aka Blind XPath Injection)	18-Oct-2022	5.3	An XPath Injection vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22244**	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5231
XML Injection (aka Blind XPath Injection)	18-Oct-2022	4.3	An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper Networks Junos OS allows an authenticated	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to add an XPath command to the XPath stream, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22243**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2022	4.3	A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built into Junos OS. The attacker should not be	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to execute the file due to validation checks built into Junos OS. Successful exploitation of this vulnerability could lead to loss of filesystem integrity. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22245**		
Affected Version(s): 21.2					
Deserialization of Untrusted Data	18-Oct-2022	9.8	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST request, deserialization may occur which could lead to unauthorized	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local file access or the ability to execute arbitrary commands. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22241**		
Inclusion of Functionality from Untrusted Control Sphere	18-Oct-2022	8.8	A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By chaining this vulnerability with other unspecified vulnerabilities, and by circumventing existing attack requirements, successful exploitation	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to a complete system compromise. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22246**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a	https://kb.juniper.net/JSA69900	O-JUN-JUNO-071122/5236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malformed ESP packet matching an established IPsec tunnel is received the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to	https://kb.juniper.net/JSA69901	O-JUN-JUNO-071122/5237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and	https://kb.juniper.net/JSA69873	O-JUN-JUNO-071122/5238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IPv6 packets. Packets of either type can cause and sustain the DoS event. These packets can be destined to the device or be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 |		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			refresh 1 | no-more and reviewing for backpressured output; for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Type of Input vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS allows an attacker to cause an RPD memory leak leading to a Denial of Service (DoS). This memory leak only occurs	https://kb.juniper.net/JSA69880	O-JUN-JUNO-071122/5239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when the attacker's packets are destined to any configured IPv6 address on the device. This issue affects: Juniper Networks Junos OS 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. **CVE ID : CVE-2022-22228**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will	https://kb.juniper.net/JSA69891	O-JUN-JUNO-071122/5240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1	https://kb.juniper.net/JSA69892	O-JUN-JUNO-071122/5241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Authentication	18-Oct-2022	6.5	An Improper Authentication vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause an impact on confidentiality or integrity. A vulnerability in the processing of TCP-AO will allow a BGP or LDP peer not configured with authentication to	https://kb.juniper.net/JSA69893	O-JUN-JUNO-071122/5243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			establish a session even if the peer is locally configured to use authentication. This could lead to untrusted or unauthorized sessions being established. This issue affects Juniper Networks Junos OS: 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS Evolved. **CVE ID : CVE-2022-22237**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between	https://kb.juniper.net/JSA69906	O-JUN-JUNO-071122/5245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			two local interfaces or between core/EVPN and local interface. The below error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site Scripting (XSS) vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker to run malicious scripts reflected off of J-Web to the victim's browser in the context of their session within J-Web. This issue affects Juniper Networks Junos OS all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.4R2; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2022-22242**		
Use After Free	18-Oct-2022	5.9	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause Denial of Service (DoS). When a BGP session flap happens, a Use After Free of a memory location that was assigned to another object can occur, which will lead to an rpd crash. This is a race condition that is outside of the attacker's control and cannot be deterministically exploited. Continued flapping of BGP sessions can create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 version 19.2R1 and later versions; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-	https://kb.juniper.net/JSA69879	O-JUN-JUNO-071122/5248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22208**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated attacker with an established BGP session to cause a Denial of Service (DoS). In a BGP multipath scenario, when one of the contributing routes is flapping often and rapidly, rpd may crash. As this crash depends on whether a route is a contributing route, and on the internal timing of the events triggered by the flap this vulnerability is outside the direct control of a potential attacker. This issue affects: Juniper	https://kb.juniper.net/JSA69875	O-JUN-JUNO-071122/5249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS 19.2 versions prior to 19.2R3-S6; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R2-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions 19.2 versions prior to 19.2R2, 19.3R1 and above prior to 20.2R1. Juniper Networks Junos OS Evolved versions prior to 20.2R1-EVO. **CVE ID : CVE-2022-22225**		
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to	https://kb.juniper.net/JSA69890	O-JUN-JUNO-071122/5250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged %PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Missing Release of Memory after Effective Lifetime	18-Oct-2022	5.5	An Allocation of Resources Without Limits or Throttling and a Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated low privileged attacker to cause a Denial of Sevice (DoS). In a high-scaled BGP routing	https://kb.juniper.net/JSA69896	O-JUN-JUNO-071122/5251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			environment with rib-sharding enabled, two issues may occur when executing a specific CLI command. One is a memory leak issue with rpd where the leak rate is not constant, and the other is a temporary spike in rpd memory usage during command execution. This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R1-S2-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. **CVE ID : CVE-2022-22240**		
XML Injection (aka Blind	18-Oct-2022	5.3	An XPath Injection vulnerability in the J-Web component of	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
XPath Injection)			Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22244**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	4.3	An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to add an XPath command to the XPath stream, which may allow	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22243**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2022	4.3	A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built into Junos OS. The attacker should not be able to execute the file due to validation checks built into Junos OS.	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability could lead to loss of filesystem integrity. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22245**		
Affected Version(s): 21.3					
Deserialization of Untrusted Data	18-Oct-2022	9.8	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST request, deserialization may occur which could lead to unauthorized local file access or the ability to execute arbitrary commands.	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22241**		
Inclusion of Functionality from Untrusted Control Sphere	18-Oct-2022	8.8	A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By chaining this vulnerability with other unspecified vulnerabilities, and by circumventing existing attack requirements, successful exploitation could lead to a complete system compromise. This issue affects Juniper	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22246**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). On SRX5000 Series with SPC3, SRX4000 Series, and vSRX, when PowerMode IPsec is configured and a malformed ESP packet matching an established IPsec tunnel is received	https://kb.juniper.net/JSA69900	O-JUN-JUNO-071122/5257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the PFE crashes. This issue affects Juniper Networks Junos OS on SRX5000 Series with SPC3, SRX4000 Series, and vSRX: All versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. **CVE ID : CVE-2022-22201**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on	https://kb.juniper.net/JSA69901	O-JUN-JUNO-071122/5258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SRX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
Improper Input Validation	18-Oct-2022	7.5	On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition. Continued receipt and processing of these packets will sustain the Denial of Service. This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event.	https://kb.juniper.net/JSA69873	O-JUN-JUNO-071122/5259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These packets can be destined to the device or be transit packets. On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service. This issue affects: Juniper Networks Junos OS on QFX10000 Series: All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S1. An indicator of compromise may be seen by issuing the command: request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more and reviewing for backpressured output;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for example: GOT: 0x220702a8 pe.ps.l2_node[10].pkt_cnt 00000076 GOT: 0x220702b4 pe.ps.l2_node[10].backpressured 00000002 <<<< STICKS HERE and requesting detail on the pepic wanio: request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2 GOT: 3 xe-0/0/0:2 10 6 3 0 1 10 189 10 0x6321b088 <<< LOOK HERE as well as looking for tail drops looking at the interface queue, for example: show interfaces queue xe-0/0/0:2 resulting in: Transmitted: Total-dropped packets: 1094137 0 pps << LOOK HERE **CVE ID : CVE-2022-22223**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Type of Input vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS allows an attacker to cause an RPD memory leak leading to a Denial of Service (DoS). This memory leak only occurs when the attacker's packets are destined to any configured IPv6	https://kb.juniper.net/JSA69880	O-JUN-JUNO-071122/5260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address on the device. This issue affects: Juniper Networks Junos OS 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. **CVE ID : CVE-2022-22228**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled.	https://kb.juniper.net/JSA69891	O-JUN-JUNO-071122/5261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions	https://kb.juniper.net/JSA69892	O-JUN-JUNO-071122/5262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Authentication	18-Oct-2022	6.5	An Improper Authentication vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause an impact on confidentiality or integrity. A vulnerability in the processing of TCP-AO will allow a BGP or LDP peer not configured with authentication to establish a session even if the peer is locally configured to use	https://kb.juniper.net/JSA69893	O-JUN-JUNO-071122/5264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication. This could lead to untrusted or unauthorized sessions being established. This issue affects Juniper Networks Junos OS: 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS Evolved. **CVE ID : CVE-2022-22237**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface. The below	https://kb.juniper.net/JSA69906	O-JUN-JUNO-071122/5266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			error logs can be seen in PFE syslog when this issue happens: xss_event_handler(1071) : EA[0:0]_PPE 46.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 1.xss[0] ADDR Error. ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error xss_event_handler(1071) : EA[0:0]_PPE 2.xss[0] ADDR Error. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 15.1R7-S13; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. **CVE ID : CVE-2022-22249**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	A Cross-site Scripting (XSS) vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker to run malicious scripts reflected off of J-Web to the victim's browser in the context of their session within J-Web. This issue affects Juniper Networks Junos OS all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2022-22242**	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2022	5.9	Due to the Improper Handling of an Unexpected Data Type in the processing of EVPN routes on Juniper Networks Junos OS and Junos OS Evolved, an attacker in direct control of a BGP client connected to a route reflector, or via a machine in the middle (MITM) attack, can send a specific EVPN route contained within a BGP Update, triggering a routing protocol daemon (RPD) crash, leading to a Denial of Service (DoS) condition. Continued receipt and processing of these specific EVPN routes could create a sustained Denial of Service (DoS) condition. This issue only occurs on BGP route reflectors, only within a BGP EVPN multicast environment, and only when one or more BGP clients have 'leave-sync-route-oldstyle' enabled. This issue affects: Juniper Networks Junos OS 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2-S2, 21.4R3; 22.1 versions prior to 22.1R1-S2, 22.1R3; 22.2 versions prior to 22.2R2. Juniper Networks Junos OS Evolved 21.3 version 21.3R1-EVO and later versions prior to 21.4R3-	https://kb.juniper.net/JSA69898, https://www.juniper.net/documentation/us/en/software/junos/evpn-vxlan/topics/ref/statement/evpn-edit-routing-instances-protocols.html	O-JUN-JUNO-071122/5269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EVO; 22.1 versions prior to 22.1R1-S2-EVO, 22.1R3-EVO; 22.2 versions prior to 22.2R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.3R1. Juniper Networks Junos OS Evolved versions prior to 21.3R1-EVO. **CVE ID : CVE-2022-22219**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated attacker with an established BGP session to cause a Denial of Service (DoS). In a BGP multipath scenario, when one of the contributing routes is flapping often and rapidly, rpd may crash. As this crash depends on whether a route is a contributing route, and on the internal timing of the events triggered by the flap this vulnerability is outside the direct control of a potential attacker. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 20.2 versions prior to 20.2R3-S4; 20.3 versions	https://kb.juniper.net/JSA69875	O-JUN-JUNO-071122/5270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R2-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions 19.2 versions prior to 19.2R2, 19.3R1 and above prior to 20.2R1. Juniper Networks Junos OS Evolved versions prior to 20.2R1-EVO. **CVE ID : CVE-2022-22225**		
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series	https://kb.juniper.net/JSA69890	O-JUN-JUNO-071122/5271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands: user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged %PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22234**		
Missing Release of Memory after Effective Lifetime	18-Oct-2022	5.5	An Allocation of Resources Without Limits or Throttling and a Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated low privileged attacker to cause a Denial of Sevice (DoS). In a high-scaled BGP routing environment with rib-sharding enabled, two issues may occur when executing a specific CLI	https://kb.juniper.net/JSA69896	O-JUN-JUNO-071122/5272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command. One is a memory leak issue with rpd where the leak rate is not constant, and the other is a temporary spike in rpd memory usage during command execution. This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R1-S2-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. **CVE ID : CVE-2022-22240**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	5.3	An XPath Injection vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22244**		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	4.3	An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to add an XPath command to the XPath stream, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22243**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2022	4.3	A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built into Junos OS. The attacker should not be able to execute the file due to validation checks built into Junos OS. Successful exploitation of this vulnerability could lead to loss of filesystem integrity. This issue	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22245**		
Affected Version(s): 21.4					
Deserialization of Untrusted Data	18-Oct-2022	9.8	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST request, deserialization may occur which could lead to unauthorized local file access or the ability to execute arbitrary commands. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22241**		
Inclusion of Functionality from Untrusted Control Sphere	18-Oct-2022	8.8	A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By chaining this vulnerability with other unspecified vulnerabilities, and by circumventing existing attack requirements, successful exploitation could lead to a complete system compromise. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22246**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	On SRX Series devices, an Improper Check for Unusual or Exceptional Conditions when using Certificate Management Protocol Version 2 (CMPv2) auto re-enrollment, allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS) by crashing the pkid process. The pkid process cannot handle an unexpected response from the Certificate Authority (CA) server, leading to crash. A restart is required to restore services. This issue affects: Juniper Networks Junos OS on SRX Series: All versions	https://kb.juniper.net/JSA69901	O-JUN-JUNO-071122/5278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2022-22218**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Type of Input vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS allows an attacker to cause an RPD memory leak leading to a Denial of Service (DoS). This memory leak only occurs when the attacker's packets are destined to any configured IPv6 address on the device. This issue affects: Juniper Networks Junos OS 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1.	https://kb.juniper.net/JSA69880	O-JUN-JUNO-071122/5279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22228		
NULL Pointer Dereference	18-Oct-2022	7.5	An Unchecked Return Value to NULL Pointer Dereference vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series if Unified Threat Management (UTM) Enhanced Content Filtering (CF) and AntiVirus (AV) are enabled together and the system processes specific valid transit traffic the Packet Forwarding Engine (PFE) will crash and restart. This issue affects Juniper Networks Junos OS 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22231**	https://kb.juniper.net/JSA69885	O-JUN-JUNO-071122/5280
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker	https://kb.juniper.net/JSA69886	O-JUN-JUNO-071122/5281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1. **CVE ID : CVE-2022-22232**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers	https://kb.juniper.net/JSA69891	O-JUN-JUNO-071122/5282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on	https://kb.juniper.net/JSA69892	O-JUN-JUNO-071122/5283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**		
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Authentication	18-Oct-2022	6.5	An Improper Authentication vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause an impact on confidentiality or integrity. A vulnerability in the processing of TCP-	https://kb.juniper.net/JSA69893	O-JUN-JUNO-071122/5285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AO will allow a BGP or LDP peer not configured with authentication to establish a session even if the peer is locally configured to use authentication. This could lead to untrusted or unauthorized sessions being established. This issue affects Juniper Networks Junos OS: 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS Evolved. **CVE ID : CVE-2022-22237**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Improper Neutralization of Input During	18-Oct-2022	6.1	A Cross-site Scripting (XSS) vulnerability in the J-Web component of Juniper Networks Junos OS allows an	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			unauthenticated attacker to run malicious scripts reflected off of J-Web to the victim's browser in the context of their session within J-Web. This issue affects Juniper Networks Junos OS all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2022-22242**		
N/A	18-Oct-2022	5.9	Due to the Improper Handling of an Unexpected Data Type in the processing of EVPN routes on Juniper Networks Junos OS and Junos OS Evolved, an attacker in direct control of a BGP client connected to a route reflector, or via a machine in the middle (MITM) attack, can send a specific EVPN route contained within a BGP Update, triggering a	https://kb.juniper.net/JSA69898, https://www.juniper.net/documentation/us/en/software/junos/evpn-vxlan/topics/ref/statement/evpn-edit-routing-instances-	O-JUN-JUNO-071122/5288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			routing protocol daemon (RPD) crash, leading to a Denial of Service (DoS) condition. Continued receipt and processing of these specific EVPN routes could create a sustained Denial of Service (DoS) condition. This issue only occurs on BGP route reflectors, only within a BGP EVPN multicast environment, and only when one or more BGP clients have 'leave-sync-route-oldstyle' enabled. This issue affects: Juniper Networks Junos OS 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2-S2, 21.4R3; 22.1 versions prior to 22.1R1-S2, 22.1R3; 22.2 versions prior to 22.2R2. Juniper Networks Junos OS Evolved 21.3 version 21.3R1-EVO and later versions prior to 21.4R3-EVO; 22.1 versions prior to 22.1R1-S2-EVO, 22.1R3-EVO; 22.2 versions prior to 22.2R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.3R1. Juniper Networks Junos OS Evolved versions prior to 21.3R1-EVO. **CVE ID : CVE-2022-22219**	protocols.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	18-Oct-2022	5.5	An Unchecked Return Value to NULL Pointer Dereference vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). In Segment Routing (SR) to Label Distribution Protocol (LDP) interworking scenario, configured with Segment Routing Mapping Server (SRMS) at any node, when an Area Border Router (ABR) leaks the SRMS entries having "S" flag set from IS-IS Level 2 to Level 1, an rpd core might be observed when a specific low privileged CLI command is issued. This issue affects: Juniper Networks Junos OS 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R2. Juniper Networks Junos OS Evolved 21.4-EVO versions prior to 21.4R1-S2-EVO, 21.4R2-S1-EVO, 21.4R3-EVO; 22.1-EVO versions prior to 22.1R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.4R1. Juniper Networks Junos OS	https://kb.juniper.net/JSA69887	O-JUN-JUNO-071122/5289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Evolved versions prior to 21.4R1-EVO. **CVE ID : CVE-2022-22233**		
N/A	18-Oct-2022	5.5	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). If the device is very busy for example while executing a series of show commands on the CLI one or more SFPs might not be detected anymore. The system then changes its state to "unplugged" which is leading to traffic impact and at least a partial DoS. Once the system is less busy the port states return to their actual value. Indicators of compromise are log messages about unplugged SFPs and corresponding syspld messages without any physical or environmental cause. These can be checked by issuing the following commands:	https://kb.juniper.net/JSA69890	O-JUN-JUNO-071122/5290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user@device# show log messages | match unplugged %PFE-6: fpc0 sfp-0/1/2 SFP unplugged %PFE-6: fpc0 sfp-0/1/3 SFP unplugged The following log messages will also be seen when this issue happens: fpc0 Error tvp_drv_syspld_read: syspld read failed for address <address> fpc0 Error[-1]:tvp_optics_presence_get - Syspld read failed for port <pic/port> fpc0 optics pres failed(-1) for pic <pic> port <port> fpc0 tvp_drv_syspld_read: i2c access retry count 200 This issue affects Juniper Networks Junos OS on EX2300 Series, EX3400 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22234		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	5.3	An XPath Injection vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22244**	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5291
XML Injection (aka Blind XPath Injection)	18-Oct-2022	4.3	An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS allows an authenticated attacker to add an XPath command to the XPath stream, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22243**		
Improper Limitation of a Pathname to a Restricted Directory ('Path	18-Oct-2022	4.3	A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Traversal')			into Junos OS. The attacker should not be able to execute the file due to validation checks built into Junos OS. Successful exploitation of this vulnerability could lead to loss of filesystem integrity. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22245**		
Affected Version(s): 22.1					
Deserialization of Untrusted Data	18-Oct-2022	9.8	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST request, deserialization	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may occur which could lead to unauthorized local file access or the ability to execute arbitrary commands. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22241**		
Inclusion of Functionality from Untrusted Control Sphere	18-Oct-2022	8.8	A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By chaining this vulnerability with other unspecified vulnerabilities, and by circumventing existing	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack requirements, successful exploitation could lead to a complete system compromise. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22246**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Specified Type of Input vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS allows an attacker to cause an RPD memory leak leading to a Denial of Service (DoS). This memory leak only occurs when the attacker's packets are destined to any configured IPv6 address on the device.	https://kb.juniper.net/JSA69880	O-JUN-JUNO-071122/5296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects: Juniper Networks Junos OS 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. **CVE ID : CVE-2022-22228**		
NULL Pointer Dereference	18-Oct-2022	7.5	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On SRX Series If Unified Threat Management (UTM) Enhanced Content Filtering (CF) is enabled and specific transit traffic is processed the PFE will crash and restart. This issue affects Juniper Networks Junos OS: 21.4 versions prior to 21.4R1-S2, 21.4R2 on SRX Series; 22.1 versions prior to 22.1R1-S1, 22.1R2 on SRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 21.4R1.	https://kb.juniper.net/JSA69886	O-JUN-JUNO-071122/5297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22232		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	7.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based, attacker to cause Denial of Service (DoS). A PFE crash will happen when a GPRS Tunnel Protocol (GTP) packet is received with a malformed field in the IP header of GTP encapsulated General Packet Radio Services (GPRS) traffic. The packet needs to match existing state which is outside the attackers control, so the issue cannot be directly exploited. The issue will only be observed when endpoint address validation is enabled. This issue affects Juniper Networks Junos OS on SRX Series: 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1,	https://kb.juniper.net/JSA69891	O-JUN-JUNO-071122/5298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1. **CVE ID : CVE-2022-22235**		
Access of Uninitialized Pointer	18-Oct-2022	7.5	An Access of Uninitialized Pointer vulnerability in SIP Application Layer Gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When specific valid SIP packets are received the PFE will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series and MX Series: 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22236**	https://kb.juniper.net/JSA69892	O-JUN-JUNO-071122/5299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	18-Oct-2022	6.5	An Improper Authentication vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause an impact on confidentiality or integrity. A vulnerability in the processing of TCP-AO will allow a BGP or LDP peer not configured with authentication to establish a session even if the peer is locally configured to use authentication. This could lead to untrusted or unauthorized sessions being established. This issue affects Juniper Networks Junos OS: 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. This issue does not affect Juniper Networks Junos OS Evolved. **CVE ID : CVE-2022-22237**	https://kb.juniper.net/JSA69893	O-JUN-JUNO-071122/5300
Improper Neutralization of Input During Web Page Generatio	18-Oct-2022	6.1	A Cross-site Scripting (XSS) vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker to run malicious scripts	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n ('Cross-site Scripting')			reflected off of J-Web to the victim's browser in the context of their session within J-Web. This issue affects Juniper Networks Junos OS all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2022-22242**		
N/A	18-Oct-2022	5.9	Due to the Improper Handling of an Unexpected Data Type in the processing of EVPN routes on Juniper Networks Junos OS and Junos OS Evolved, an attacker in direct control of a BGP client connected to a route reflector, or via a machine in the middle (MITM) attack, can send a specific EVPN route contained within a BGP Update, triggering a routing protocol daemon (RPD) crash, leading to a	https://kb.juniper.net/JSA69898, https://www.juniper.net/documentation/us/en/software/junos/evpn-vxlan/topics/ref/statement/evpn-edit-routing-instances-protocols.html	O-JUN-JUNO-071122/5302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS) condition. Continued receipt and processing of these specific EVPN routes could create a sustained Denial of Service (DoS) condition. This issue only occurs on BGP route reflectors, only within a BGP EVPN multicast environment, and only when one or more BGP clients have 'leave-sync-route-oldstyle' enabled. This issue affects: Juniper Networks Junos OS 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2-S2, 21.4R3; 22.1 versions prior to 22.1R1-S2, 22.1R3; 22.2 versions prior to 22.2R2. Juniper Networks Junos OS Evolved 21.3 version 21.3R1-EVO and later versions prior to 21.4R3-EVO; 22.1 versions prior to 22.1R1-S2-EVO, 22.1R3-EVO; 22.2 versions prior to 22.2R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.3R1. Juniper Networks Junos OS Evolved versions prior to 21.3R1-EVO. **CVE ID : CVE-2022-22219**		
NULL Pointer	18-Oct-2022	5.5	An Unchecked Return Value to NULL Pointer Dereference	https://kb.juniper.net/JSA69887	O-JUN-JUNO-071122/5303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferen ce			vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). In Segment Routing (SR) to Label Distribution Protocol (LDP) interworking scenario, configured with Segment Routing Mapping Server (SRMS) at any node, when an Area Border Router (ABR) leaks the SRMS entries having "S" flag set from IS-IS Level 2 to Level 1, an rpd core might be observed when a specific low privileged CLI command is issued. This issue affects: Juniper Networks Junos OS 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R2. Juniper Networks Junos OS Evolved 21.4-EVO versions prior to 21.4R1-S2-EVO, 21.4R2-S1-EVO, 21.4R3-EVO; 22.1-EVO versions prior to 22.1R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.4R1. Juniper Networks Junos OS Evolved versions prior to 21.4R1-EVO.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22233		
XML Injection (aka Blind XPath Injection)	18-Oct-2022	5.3	An XPath Injection vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22244**	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5304
XML Injection (aka Blind XPath Injection)	18-Oct-2022	4.3	An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS allows an authenticated attacker to add an XPath command to the XPath stream, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22243**		
Improper Limitation of a Pathname to a Restricted Directory ('Path	18-Oct-2022	4.3	A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built	https://kb.juniper.net/JSA69899	O-JUN-JUNO-071122/5306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Traversal')			into Junos OS. The attacker should not be able to execute the file due to validation checks built into Junos OS. Successful exploitation of this vulnerability could lead to loss of filesystem integrity. This issue affects Juniper Networks Junos OS: all versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3-S5; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R2-S2, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S1, 22.1R2. **CVE ID : CVE-2022-22245**		
Affected Version(s): 22.2					
N/A	18-Oct-2022	5.9	Due to the Improper Handling of an Unexpected Data Type in the processing of EVPN routes on Juniper Networks Junos OS and Junos OS Evolved, an attacker in direct control of a BGP client connected to a route reflector, or via	https://kb.juniper.net/JSA69898, https://www.juniper.net/documentation/us/en/software/junos/evpn-vxlan/topics	O-JUN-JUNO-071122/5307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a machine in the middle (MITM) attack, can send a specific EVPN route contained within a BGP Update, triggering a routing protocol daemon (RPD) crash, leading to a Denial of Service (DoS) condition. Continued receipt and processing of these specific EVPN routes could create a sustained Denial of Service (DoS) condition. This issue only occurs on BGP route reflectors, only within a BGP EVPN multicast environment, and only when one or more BGP clients have 'leave-sync-route-oldstyle' enabled. This issue affects: Juniper Networks Junos OS 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2-S2, 21.4R3; 22.1 versions prior to 22.1R1-S2, 22.1R3; 22.2 versions prior to 22.2R2. Juniper Networks Junos OS Evolved 21.3 version 21.3R1-EVO and later versions prior to 21.4R3-EVO; 22.1 versions prior to 22.1R1-S2-EVO, 22.1R3-EVO; 22.2 versions prior to 22.2R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.3R1. Juniper Networks Junos OS	/ref/statement/evpn-edit-routing-instances-protocols.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Evolved versions prior to 21.3R1-EVO. **CVE ID : CVE-2022-22219**		
Affected Version(s): From (including) 20.2 Up to (excluding) 21.2					
Insufficiently Protected Credentials	18-Oct-2022	7.8	On cSRX Series devices software permission issues in the container filesystem and stored files combined with storing passwords in a recoverable format in Juniper Networks Junos OS allows a local, low-privileged attacker to elevate their permissions to take control of any instance of a cSRX software deployment. This issue affects Juniper Networks Junos OS 20.2 version 20.2R1 and later versions prior to 21.2R1 on cSRX Series. **CVE ID : CVE-2022-22251**	https://kb.juniper.net/JSA69908	O-JUN-JUNO-071122/5308
Product: junos_os_evolved					
Affected Version(s): 18.3					
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 19.1					
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Affected Version(s): 19.2					
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Affected Version(s): 19.3					
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22230		
Affected Version(s): 19.4					
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO;	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Affected Version(s): 20.1					
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8,	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Affected Version(s): 20.2					
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
Affected Version(s): 20.3					
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
Affected Version(s): 20.4					
Improper Privilege Management	18-Oct-2022	8.8	An Execution with Unnecessary Privileges vulnerability in Management Daemon (mgd) of Juniper Networks Junos OS Evolved allows a locally authenticated attacker with low privileges to escalate their privileges on the device and	https://kb.juniper.net/JSA69895	O-JUN-JUNO-071122/5319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially remote systems. This vulnerability allows a locally authenticated attacker with access to the ssh operational command to escalate their privileges on the system to root, or if there is user interaction on the local device to potentially escalate privileges on a remote system to root. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-EVO; 21.2-EVO versions prior to 21.2R2-S1-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS. **CVE ID : CVE-2022-22239**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Syntactic Correctness of Input vulnerability in the kernel of Juniper Networks Junos OS Evolved on PTX series allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). When an incoming TCP packet destined to the device is malformed there is a possibility of a kernel panic. Only TCP packets	https://kb.juniper.net/JSA69915	O-JUN-JUNO-071122/5320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			destined to the ports for BGP, LDP and MSDP can trigger this. This issue only affects PTX10004, PTX10008, PTX10016. No other PTX Series devices or other platforms are affected. This issue affects Juniper Networks Junos OS Evolved: 20.4-EVO versions prior to 20.4R3-S4-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 20.4R1-EVO. **CVE ID : CVE-2022-22192**		
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is	https://kb.juniper.net/JSA69916	O-JUN-JUNO-071122/5321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Incorrect Permission Assignment for	18-Oct-2022	7.3	An Incorrect Permission Assignment vulnerability in shell processing of Juniper Networks Junos OS Evolved allows a low-	https://kb.juniper.net/JSA69905	O-JUN-JUNO-071122/5322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			privileged local user to modify the contents of a configuration file which could cause another user to execute arbitrary commands within the context of the follow-on user's session. If the follow-on user is a high-privileged administrator, the attacker could leverage this vulnerability to take complete control of the target system. While this issue is triggered by a user, other than the attacker, accessing the Junos shell, an attacker simply requires Junos CLI access to exploit this vulnerability. This issue affects Juniper Networks Junos OS Evolved: 20.4-EVO versions prior to 20.4R3-S1-EVO; All versions of 21.1-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2022-22248**		
N/A	18-Oct-2022	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in the processing of a malformed OSPF TLV in Juniper Networks Junos	https://kb.juniper.net/JSA69874	O-JUN-JUNO-071122/5323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause the periodic packet management daemon (PPMD) process to go into an infinite loop, which in turn can cause protocols and functions reliant on PPMD such as OSPF neighbor reachability to be impacted, resulting in a sustained Denial of Service (DoS) condition. The DoS condition persists until the PPMD process is manually restarted. This issue affects: Juniper Networks Junos OS: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S3-EVO; 21.1 versions prior to 21.1R2-EVO. **CVE ID : CVE-2022-22224**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS, Junos OS Evolved allows a network-based unauthenticated attacker to cause a Denial of	https://kb.juniper.net/JSA69902	O-JUN-JUNO-071122/5327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS). When a BGP flow route with redirect IP extended community is received, and the reachability to the next-hop of the corresponding redirect IP is flapping, the rpd process might crash. Whether the crash occurs depends on the timing of the internally processing of these two events and is outside the attackers control. Please note that this issue also affects Route-Reflectors unless 'routing-options flow firewall-install-disable' is configured. This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.4 versions prior to 19.4R3-S8; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22220		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated attacker with an established BGP session to cause a Denial of Service (DoS). In a BGP multipath scenario, when one of the contributing routes is flapping often and rapidly, rpd may crash. As this crash depends on whether a route is a contributing route, and on the internal timing of the events triggered by the flap this vulnerability is outside the direct control of a potential attacker. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO	https://kb.juniper.net/JSA69875	O-JUN-JUNO-071122/5328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.2R2-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions 19.2 versions prior to 19.2R2, 19.3R1 and above prior to 20.2R1. Juniper Networks Junos OS Evolved versions prior to 20.2R1-EVO. **CVE ID : CVE-2022-22225**		
Missing Release of Memory after Effective Lifetime	18-Oct-2022	5.5	An Allocation of Resources Without Limits or Throttling and a Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated low privileged attacker to cause a Denial of Sevice (DoS). In a high-scaled BGP routing environment with rib-sharding enabled, two issues may occur when executing a specific CLI command. One is a memory leak issue with rpd where the leak rate is not constant, and the other is a temporary spike in rpd memory usage during command execution. This issue affects: Juniper Networks Junos OS 19.4 versions	https://kb.juniper.net/JSA69896	O-JUN-JUNO-071122/5329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R1-S2-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. **CVE ID : CVE-2022-22240**		
Affected Version(s): 21.1					
Improper Privilege Management	18-Oct-2022	8.8	An Execution with Unnecessary Privileges vulnerability in Management Daemon (mgd) of Juniper Networks Junos OS Evolved allows a locally authenticated attacker with low privileges to escalate their privileges on the device and potentially remote systems. This vulnerability allows a locally authenticated attacker with access to	https://kb.juniper.net/JSA69895	O-JUN-JUNO-071122/5330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the ssh operational command to escalate their privileges on the system to root, or if there is user interaction on the local device to potentially escalate privileges on a remote system to root. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-EVO; 21.2-EVO versions prior to 21.2R2-S1-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS. **CVE ID : CVE-2022-22239**		
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-	https://kb.juniper.net/JSA69916	O-JUN-JUNO-071122/5331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVEN		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			T: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Incorrect Permission Assignment for	18-Oct-2022	7.3	An Incorrect Permission Assignment vulnerability in shell processing of Juniper Networks Junos OS Evolved allows a low-privileged local user to	https://kb.juniper.net/JSA69905	O-JUN-JUNO-071122/5332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			modify the contents of a configuration file which could cause another user to execute arbitrary commands within the context of the follow-on user's session. If the follow-on user is a high-privileged administrator, the attacker could leverage this vulnerability to take complete control of the target system. While this issue is triggered by a user, other than the attacker, accessing the Junos shell, an attacker simply requires Junos CLI access to exploit this vulnerability. This issue affects Juniper Networks Junos OS Evolved: 20.4-EVO versions prior to 20.4R3-S1-EVO; All versions of 21.1-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2022-22248**		
N/A	18-Oct-2022	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in the processing of a malformed OSPF TLV in Juniper Networks Junos OS and Junos OS Evolved	https://kb.juniper.net/JSA69874	O-JUN-JUNO-071122/5333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows an unauthenticated adjacent attacker to cause the periodic packet management daemon (PPMD) process to go into an infinite loop, which in turn can cause protocols and functions reliant on PPMD such as OSPF neighbor reachability to be impacted, resulting in a sustained Denial of Service (DoS) condition. The DoS condition persists until the PPMD process is manually restarted. This issue affects: Juniper Networks Junos OS: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S3-EVO; 21.1 versions prior to 21.1R2-EVO. **CVE ID : CVE-2022-22224**		
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Use After Free	18-Oct-2022	5.9	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause Denial of Service (DoS). When a BGP session flap happens, a Use After Free of a memory location that	https://kb.juniper.net/JSA69879	O-JUN-JUNO-071122/5337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was assigned to another object can occur, which will lead to an rpd crash. This is a race condition that is outside of the attacker's control and cannot be deterministically exploited. Continued flapping of BGP sessions can create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 version 19.2R1 and later versions; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22208**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS, Junos OS Evolved allows a network-based unauthenticated attacker to cause a Denial of Service (DoS). When a BGP flow route with redirect IP extended community is received, and the reachability to the next-hop of the corresponding redirect IP is flapping, the rpd process might crash. Whether the crash occurs depends on the timing of the internally processing of these two events and is outside the attackers control. Please note that this issue also affects Route-Reflectors unless 'routing-options flow firewall-install-disable' is configured. This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.4 versions prior to 19.4R3-S8; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper	https://kb.juniper.net/JSA69902	O-JUN-JUNO-071122/5338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22220**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated attacker with an established BGP session to cause a Denial of Service (DoS). In a BGP multipath scenario, when one of the contributing routes is flapping often and rapidly, rpd may crash. As this crash depends on whether a route is a contributing route, and on the internal timing of the events triggered by the flap this vulnerability is outside the direct control of a potential attacker. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-	https://kb.juniper.net/JSA69875	O-JUN-JUNO-071122/5339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R2-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions 19.2 versions prior to 19.2R2, 19.3R1 and above prior to 20.2R1. Juniper Networks Junos OS Evolved versions prior to 20.2R1-EVO. **CVE ID : CVE-2022-22225**		
Missing Release of Memory after Effective Lifetime	18-Oct-2022	5.5	An Allocation of Resources Without Limits or Throttling and a Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated low privileged attacker to cause a Denial of Sevice (DoS). In a high-scaled BGP routing environment with rib-sharding enabled, two issues may occur when executing a specific CLI	https://kb.juniper.net/JSA69896	O-JUN-JUNO-071122/5340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command. One is a memory leak issue with rpd where the leak rate is not constant, and the other is a temporary spike in rpd memory usage during command execution. This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R1-S2-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. **CVE ID : CVE-2022-22240**		
Improper Check for Unusual or Exceptional	18-Oct-2022	5.3	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved on ACX7000	https://kb.juniper.net/JSA69878	O-JUN-JUNO-071122/5341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conditions			Series allows an unauthenticated network-based attacker to cause a partial Denial of Service (DoS). On receipt of specific IPv6 transit traffic, Junos OS Evolved on ACX7100-48L, ACX7100-32C and ACX7509 sends this traffic to the Routing Engine (RE) instead of forwarding it, leading to increased CPU utilization of the RE and a partial DoS. This issue only affects systems configured with IPv6. This issue does not affect ACX7024 which is supported from 22.3R1-EVO onwards where the fix has already been incorporated as indicated in the solution section. This issue affects Juniper Networks Junos OS Evolved on ACX7100-48L, ACX7100-32C, ACX7509: 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S2-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22227		
Affected Version(s): 21.2					
Improper Privilege Management	18-Oct-2022	8.8	An Execution with Unnecessary Privileges vulnerability in Management Daemon (mgd) of Juniper Networks Junos OS Evolved allows a locally authenticated attacker with low privileges to escalate their privileges on the device and potentially remote systems. This vulnerability allows a locally authenticated attacker with access to the ssh operational command to escalate their privileges on the system to root, or if there is user interaction on the local device to potentially escalate privileges on a remote system to root. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-EVO; 21.2-EVO versions prior to 21.2R2-S1-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS. **CVE ID : CVE-2022-22239**	https://kb.juniper.net/JSA69895	O-JUN-JUNO-071122/5342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai"	https://kb.juniper.net/JSA69916	O-JUN-JUNO-071122/5343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Incorrect Permission Assignment for Critical Resource	18-Oct-2022	7.3	An Incorrect Permission Assignment vulnerability in shell processing of Juniper Networks Junos OS Evolved allows a low-privileged local user to modify the contents of a configuration file which could cause another user to execute arbitrary commands within the context of the follow-on user's session. If the follow-on user is a high-privileged administrator, the attacker could leverage this vulnerability to take complete control of the target system. While this issue is triggered by a user, other than the attacker, accessing the Junos shell, an attacker simply requires Junos CLI access to exploit this vulnerability. This issue affects Juniper Networks Junos OS Evolved: 20.4-EVO versions prior to	https://kb.juniper.net/JSA69905	O-JUN-JUNO-071122/5344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.4R3-S1-EVO; All versions of 21.1-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2022-22248**		
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core.	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22250		
Use After Free	18-Oct-2022	5.9	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause Denial of Service (DoS). When a BGP session flap happens, a Use After Free of a memory location that was assigned to another object can occur, which will lead to an rpd crash. This is a race condition that is outside of the attacker's control and cannot be deterministically exploited. Continued flapping of BGP sessions can create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 version 19.2R1 and later versions; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1	https://kb.juniper.net/JSA69879	O-JUN-JUNO-071122/5348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22208**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated attacker with an established BGP session to cause a Denial of Service (DoS). In a BGP multipath scenario, when one of the contributing routes is flapping often and rapidly, rpd may crash. As this crash depends on whether a route is a contributing route, and on the internal timing of the events triggered by the flap this vulnerability is outside the direct control of a potential attacker. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 20.2 versions prior to	https://kb.juniper.net/JSA69875	O-JUN-JUNO-071122/5349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R2-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions 19.2 versions prior to 19.2R2, 19.3R1 and above prior to 20.2R1. Juniper Networks Junos OS Evolved versions prior to 20.2R1-EVO. **CVE ID : CVE-2022-22225**		
Missing Release of Memory after Effective Lifetime	18-Oct-2022	5.5	An Allocation of Resources Without Limits or Throttling and a Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated low privileged attacker to cause a Denial of Sevice (DoS). In a high-scaled BGP routing environment with rib-	https://kb.juniper.net/JSA69896	O-JUN-JUNO-071122/5350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sharding enabled, two issues may occur when executing a specific CLI command. One is a memory leak issue with rpd where the leak rate is not constant, and the other is a temporary spike in rpd memory usage during command execution. This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R1-S2-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. **CVE ID : CVE-2022-22240**		
Improper Check for Unusual or	18-Oct-2022	5.3	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding	https://kb.juniper.net/JSA69878	O-JUN-JUNO-071122/5351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			Engine (PFE) of Juniper Networks Junos OS Evolved on ACX7000 Series allows an unauthenticated network-based attacker to cause a partial Denial of Service (DoS). On receipt of specific IPv6 transit traffic, Junos OS Evolved on ACX7100-48L, ACX7100-32C and ACX7509 sends this traffic to the Routing Engine (RE) instead of forwarding it, leading to increased CPU utilization of the RE and a partial DoS. This issue only affects systems configured with IPv6. This issue does not affect ACX7024 which is supported from 22.3R1-EVO onwards where the fix has already been incorporated as indicated in the solution section. This issue affects Juniper Networks Junos OS Evolved on ACX7100-48L, ACX7100-32C, ACX7509: 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S2-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2022-22227**		
Affected Version(s): 21.3					
Improper Privilege Management	18-Oct-2022	8.8	An Execution with Unnecessary Privileges vulnerability in Management Daemon (mgd) of Juniper Networks Junos OS Evolved allows a locally authenticated attacker with low privileges to escalate their privileges on the device and potentially remote systems. This vulnerability allows a locally authenticated attacker with access to the ssh operational command to escalate their privileges on the system to root, or if there is user interaction on the local device to potentially escalate privileges on a remote system to root. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-EVO; 21.2-EVO versions prior to 21.2R2-S1-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS.	https://kb.juniper.net/JSA69895	O-JUN-JUNO-071122/5352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22239		
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Syntactic Correctness of Input vulnerability in the kernel of Juniper Networks Junos OS Evolved on PTX series allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). When an incoming TCP packet destined to the device is malformed there is a possibility of a kernel panic. Only TCP packets destined to the ports for BGP, LDP and MSDP can trigger this. This issue only affects PTX10004, PTX10008, PTX10016. No other PTX Series devices or other platforms are affected. This issue affects Juniper Networks Junos OS Evolved: 20.4-EVO versions prior to 20.4R3-S4-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 20.4R1-EVO. **CVE ID : CVE-2022-22192**	https://kb.juniper.net/JSA69915	O-JUN-JUNO-071122/5353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai"	https://kb.juniper.net/JSA69916	O-JUN-JUNO-071122/5354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Input Validation vulnerability in ingress TCP segment processing of Juniper Networks Junos OS Evolved allows a network-based unauthenticated attacker to send a crafted TCP segment to the device, triggering a kernel panic, leading to a Denial of Service (DoS) condition. Continued receipt and processing of this TCP segment could create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS Evolved: 21.3 versions prior to 21.3R3-EVO; 21.4 versions prior to 21.4R2-EVO; 22.1 versions prior to 22.1R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.3R1-EVO.	https://kb.juniper.net/JSA69904	O-JUN-JUNO-071122/5355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22247		
Incorrect Permission Assignment for Critical Resource	18-Oct-2022	7.3	An Incorrect Permission Assignment vulnerability in shell processing of Juniper Networks Junos OS Evolved allows a low-privileged local user to modify the contents of a configuration file which could cause another user to execute arbitrary commands within the context of the follow-on user's session. If the follow-on user is a high-privileged administrator, the attacker could leverage this vulnerability to take complete control of the target system. While this issue is triggered by a user, other than the attacker, accessing the Junos shell, an attacker simply requires Junos CLI access to exploit this vulnerability. This issue affects Juniper Networks Junos OS Evolved: 20.4-EVO versions prior to 20.4R3-S1-EVO; All versions of 21.1-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 19.2R1-EVO.	https://kb.juniper.net/JSA69905	O-JUN-JUNO-071122/5356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22248		
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Use After Free	18-Oct-2022	5.9	A Use After Free vulnerability in the Routing Protocol Daemon (rdp) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker	https://kb.juniper.net/JSA69879	O-JUN-JUNO-071122/5360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause Denial of Service (DoS). When a BGP session flap happens, a Use After Free of a memory location that was assigned to another object can occur, which will lead to an rpd crash. This is a race condition that is outside of the attacker's control and cannot be deterministically exploited. Continued flapping of BGP sessions can create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: All versions prior to 18.4R2-S9, 18.4R3-S11; 19.1 versions prior to 19.1R3-S8; 19.2 version 19.2R1 and later versions; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R2-S1, 21.2R3. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22208**		
N/A	18-Oct-2022	5.9	Due to the Improper Handling of an Unexpected Data Type in the processing of EVPN routes on Juniper Networks Junos OS and Junos OS Evolved, an attacker in direct control of a BGP client connected to a route reflector, or via a machine in the middle (MITM) attack, can send a specific EVPN route contained within a BGP Update, triggering a routing protocol daemon (RPD) crash, leading to a Denial of Service (DoS) condition. Continued receipt and processing of these specific EVPN routes could create a sustained Denial of Service (DoS) condition. This issue only occurs on BGP route reflectors, only within a BGP EVPN multicast environment, and only when one or more BGP clients have 'leave-sync-route-oldstyle' enabled. This issue affects: Juniper Networks Junos OS 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2-S2, 21.4R3; 22.1 versions prior to 22.1R1-S2, 22.1R3; 22.2 versions	https://kb.juniper.net/JSA69898, https://www.juniper.net/documentation/us/en/software/junos/evpn-vxlan/topics/ref/statement/evpn-edit-routing-instances-protocols.html	O-JUN-JUNO-071122/5361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 22.2R2. Juniper Networks Junos OS Evolved 21.3 version 21.3R1-EVO and later versions prior to 21.4R3-EVO; 22.1 versions prior to 22.1R1-S2-EVO, 22.1R3-EVO; 22.2 versions prior to 22.2R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.3R1. Juniper Networks Junos OS Evolved versions prior to 21.3R1-EVO. **CVE ID : CVE-2022-22219**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated attacker with an established BGP session to cause a Denial of Service (DoS). In a BGP multipath scenario, when one of the contributing routes is flapping often and rapidly, rpd may crash. As this crash depends on whether a route is a contributing route, and on the internal timing of the events triggered by the flap this vulnerability is outside the direct control of a potential attacker. This	https://kb.juniper.net/JSA69875	O-JUN-JUNO-071122/5362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R2-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions 19.2 versions prior to 19.2R2, 19.3R1 and above prior to 20.2R1. Juniper Networks Junos OS Evolved versions prior to 20.2R1-EVO. **CVE ID : CVE-2022-22225**		
Missing Release of Memory after Effective Lifetime	18-Oct-2022	5.5	An Allocation of Resources Without Limits or Throttling and a Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated low privileged attacker	https://kb.juniper.net/JSA69896	O-JUN-JUNO-071122/5363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause a Denial of Sevice (DoS). In a high-scaled BGP routing environment with rib-sharding enabled, two issues may occur when executing a specific CLI command. One is a memory leak issue with rpd where the leak rate is not constant, and the other is a temporary spike in rpd memory usage during command execution. This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R1-S2-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. **CVE ID : CVE-2022-22240**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	5.3	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved on ACX7000 Series allows an unauthenticated network-based attacker to cause a partial Denial of Service (DoS). On receipt of specific IPv6 transit traffic, Junos OS Evolved on ACX7100-48L, ACX7100-32C and ACX7509 sends this traffic to the Routing Engine (RE) instead of forwarding it, leading to increased CPU utilization of the RE and a partial DoS. This issue only affects systems configured with IPv6. This issue does not affect ACX7024 which is supported from 22.3R1-EVO onwards where the fix has already been incorporated as indicated in the solution section. This issue affects Juniper Networks Junos OS Evolved on ACX7100-48L, ACX7100-32C, ACX7509: 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S2-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO,	https://kb.juniper.net/JSA69878	O-JUN-JUNO-071122/5364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.4R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2022-22227**		
Affected Version(s): 21.4					
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Syntactic Correctness of Input vulnerability in the kernel of Juniper Networks Junos OS Evolved on PTX series allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). When an incoming TCP packet destined to the device is malformed there is a possibility of a kernel panic. Only TCP packets destined to the ports for BGP, LDP and MSDP can trigger this. This issue only affects PTX10004, PTX10008, PTX10016. No other PTX Series devices or other platforms are affected. This issue affects Juniper Networks Junos OS Evolved: 20.4-EVO versions prior to 20.4R3-S4-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R2-EVO. This issue does not affect Juniper Networks Junos	https://kb.juniper.net/JSA69915	O-JUN-JUNO-071122/5365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS Evolved versions prior to 20.4R1-EVO. **CVE ID : CVE-2022-22192**		
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295	https://kb.juniper.net/JSA69916	O-JUN-JUNO-071122/5366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Input Validation vulnerability in ingress TCP segment processing of Juniper Networks Junos OS Evolved allows a network-based unauthenticated attacker to send a crafted TCP segment to the device, triggering a kernel panic, leading to a Denial of Service (DoS) condition. Continued receipt and processing of this TCP segment could create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS Evolved: 21.3 versions prior to 21.3R3-EVO; 21.4 versions prior to 21.4R2-EVO; 22.1 versions prior to 22.1R2-	https://kb.juniper.net/JSA69904	O-JUN-JUNO-071122/5367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.3R1-EVO. **CVE ID : CVE-2022-22247**		
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
NULL Pointer Dereference	18-Oct-2022	5.5	An Unchecked Return Value to NULL Pointer Dereference vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally	https://kb.juniper.net/JSA69887	O-JUN-JUNO-071122/5370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker with low privileges to cause a Denial of Service (DoS). In Segment Routing (SR) to Label Distribution Protocol (LDP) interworking scenario, configured with Segment Routing Mapping Server (SRMS) at any node, when an Area Border Router (ABR) leaks the SRMS entries having "S" flag set from IS-IS Level 2 to Level 1, an rpd core might be observed when a specific low privileged CLI command is issued. This issue affects: Juniper Networks Junos OS 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R2. Juniper Networks Junos OS Evolved 21.4-EVO versions prior to 21.4R1-S2-EVO, 21.4R2-S1-EVO, 21.4R3-EVO; 22.1-EVO versions prior to 22.1R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.4R1. Juniper Networks Junos OS Evolved versions prior to 21.4R1-EVO. **CVE ID : CVE-2022-22233**		
Improper Check for Unusual	18-Oct-2022	5.3	An Improper Check for Unusual or Exceptional Conditions vulnerability	https://kb.juniper.net/JSA69878	O-JUN-JUNO-071122/5371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Exceptional Conditions			in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved on ACX7000 Series allows an unauthenticated network-based attacker to cause a partial Denial of Service (DoS). On receipt of specific IPv6 transit traffic, Junos OS Evolved on ACX7100-48L, ACX7100-32C and ACX7509 sends this traffic to the Routing Engine (RE) instead of forwarding it, leading to increased CPU utilization of the RE and a partial DoS. This issue only affects systems configured with IPv6. This issue does not affect ACX7024 which is supported from 22.3R1-EVO onwards where the fix has already been incorporated as indicated in the solution section. This issue affects Juniper Networks Junos OS Evolved on ACX7100-48L, ACX7100-32C, ACX7509: 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S2-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2022-22227**		
Affected Version(s): 22.1					
Improper Input Validation	18-Oct-2022	7.5	An Improper Validation of Syntactic Correctness of Input vulnerability in the kernel of Juniper Networks Junos OS Evolved on PTX series allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). When an incoming TCP packet destined to the device is malformed there is a possibility of a kernel panic. Only TCP packets destined to the ports for BGP, LDP and MSDP can trigger this. This issue only affects PTX10004, PTX10008, PTX10016. No other PTX Series devices or other platforms are affected. This issue affects Juniper Networks Junos OS Evolved: 20.4-EVO versions prior to 20.4R3-S4-EVO; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 20.4R1-EVO.	https://kb.juniper.net/JSA69915	O-JUN-JUNO-071122/5372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22192		
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556	https://kb.juniper.net/JSA69916	O-JUN-JUNO-071122/5373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1 sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
Improper Input Validation	18-Oct-2022	7.5	An Improper Input Validation vulnerability in ingress TCP segment processing of Juniper Networks Junos OS Evolved allows a network-based unauthenticated attacker to send a crafted TCP segment to the device, triggering a kernel panic, leading to a Denial of Service (DoS) condition. Continued receipt and processing of this TCP segment could create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS Evolved: 21.3 versions prior to 21.3R3-EVO; 21.4 versions prior to 21.4R2-EVO; 22.1 versions prior to 22.1R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved	https://kb.juniper.net/JSA69904	O-JUN-JUNO-071122/5374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.3R1-EVO. **CVE ID : CVE-2022-22247**		
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
N/A	18-Oct-2022	5.9	Due to the Improper Handling of an Unexpected Data Type in the processing of EVPN routes on Juniper Networks Junos OS and Junos OS Evolved, an attacker in direct control of a BGP client connected to a route reflector, or via a machine in the middle (MITM) attack, can send a specific EVPN route contained within a BGP Update, triggering a routing protocol daemon (RPD) crash, leading to a Denial of Service (DoS) condition. Continued receipt and processing of these specific EVPN routes could create a sustained Denial of Service (DoS) condition. This issue only occurs on	https://kb.juniper.net/JSA69898, https://www.juniper.net/documentation/us/en/software/junos/evpn-vxlan/topics/ref/statement/evpn-edit-routing-instances-protocols.html	O-JUN-JUNO-071122/5376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BGP route reflectors, only within a BGP EVPN multicast environment, and only when one or more BGP clients have 'leave-sync-route-oldstyle' enabled. This issue affects: Juniper Networks Junos OS 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2-S2, 21.4R3; 22.1 versions prior to 22.1R1-S2, 22.1R3; 22.2 versions prior to 22.2R2. Juniper Networks Junos OS Evolved 21.3 version 21.3R1-EVO and later versions prior to 21.4R3-EVO; 22.1 versions prior to 22.1R1-S2-EVO, 22.1R3-EVO; 22.2 versions prior to 22.2R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.3R1. Juniper Networks Junos OS Evolved versions prior to 21.3R1-EVO. **CVE ID : CVE-2022-22219**		
NULL Pointer Dereference	18-Oct-2022	5.5	An Unchecked Return Value to NULL Pointer Dereference vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated attacker with low privileges to cause a Denial of Service	https://kb.juniper.net/JSA69887	O-JUN-JUNO-071122/5377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS). In Segment Routing (SR) to Label Distribution Protocol (LDP) interworking scenario, configured with Segment Routing Mapping Server (SRMS) at any node, when an Area Border Router (ABR) leaks the SRMS entries having "S" flag set from IS-IS Level 2 to Level 1, an rpd core might be observed when a specific low privileged CLI command is issued. This issue affects: Juniper Networks Junos OS 21.4 versions prior to 21.4R1-S2, 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R2. Juniper Networks Junos OS Evolved 21.4-EVO versions prior to 21.4R1-S2-EVO, 21.4R2-S1-EVO, 21.4R3-EVO; 22.1-EVO versions prior to 22.1R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.4R1. Juniper Networks Junos OS Evolved versions prior to 21.4R1-EVO. **CVE ID : CVE-2022-22233**		
Affected Version(s): 22.2					
Improper Input Validation	18-Oct-2022	6.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and	https://kb.juniper.net/JSA69884	O-JUN-JUNO-071122/5378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS Evolved allows an adjacent unauthenticated attacker to cause DoS (Denial of Service). If another router generates more than one specific valid OSPFv3 LSA then rpd will crash while processing these LSAs. This issue only affects systems configured with OSPFv3, while OSPFv2 is not affected. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 19.3 version 19.3R2 and later versions; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-S2-EVO; 21.2-EVO versions prior to 21.2R3-S1-EVO; 21.3-EVO versions prior to 21.3R3-S2-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS 19.2 versions prior to 19.2R2. **CVE ID : CVE-2022-22230**		
N/A	18-Oct-2022	5.9	Due to the Improper Handling of an Unexpected Data Type in the processing of EVPN routes on Juniper Networks Junos OS and Junos OS Evolved, an attacker in direct control of a BGP client connected to a route reflector, or via a machine in the middle (MITM) attack, can send a specific EVPN route contained within a BGP Update, triggering a routing protocol daemon (RPD) crash, leading to a Denial of Service (DoS) condition. Continued receipt and processing of these specific EVPN routes could create a sustained Denial of Service (DoS) condition. This issue only occurs on BGP route reflectors, only within a BGP EVPN multicast environment, and only when one or more BGP clients have 'leave-sync-route-oldstyle' enabled. This issue affects: Juniper Networks Junos OS 21.3 versions prior to 21.3R3-	https://kb.juniper.net/JSA69898, https://www.juniper.net/documentation/us/en/software/junos/evpn-vxlan/topics/ref/statement/evpn-edit-routing-instances-protocols.html	O-JUN-JUNO-071122/5379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S2; 21.4 versions prior to 21.4R2-S2, 21.4R3; 22.1 versions prior to 22.1R1-S2, 22.1R3; 22.2 versions prior to 22.2R2. Juniper Networks Junos OS Evolved 21.3 version 21.3R1-EVO and later versions prior to 21.4R3-EVO; 22.1 versions prior to 22.1R1-S2-EVO, 22.1R3-EVO; 22.2 versions prior to 22.2R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.3R1. Juniper Networks Junos OS Evolved versions prior to 21.3R1-EVO. **CVE ID : CVE-2022-22219**		
Affected Version(s): * Up to (excluding) 20.2					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2022	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When an incoming RESV message corresponding to a protected LSP is malformed it causes an incorrect internal state resulting in an rpd core. This issue affects: Juniper Networks Junos OS All versions prior to 19.2R3-	https://kb.juniper.net/JSA69894	O-JUN-JUNO-071122/5380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.2R3-S3-EVO; 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22238**		
Affected Version(s): * Up to (excluding) 20.4					
Improper Privilege Management	18-Oct-2022	8.8	An Execution with Unnecessary Privileges vulnerability in Management Daemon (mgd) of Juniper Networks Junos OS Evolved allows a locally authenticated attacker with low privileges to escalate their privileges on the device and potentially remote systems. This	https://kb.juniper.net/JSA69895	O-JUN-JUNO-071122/5381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows a locally authenticated attacker with access to the ssh operational command to escalate their privileges on the system to root, or if there is user interaction on the local device to potentially escalate privileges on a remote system to root. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.1-EVO versions prior to 21.1R3-EVO; 21.2-EVO versions prior to 21.2R2-S1-EVO, 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS. **CVE ID : CVE-2022-22239**		
Allocation of Resources Without Limits or Throttling	18-Oct-2022	7.5	A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Continuously polling the SNMP jnxCosQstatTable causes the FPC to run out of GUID space, causing a Denial of Service to the FPC resources. When the FPC runs out of the GUID space, you will see the following syslog	https://kb.juniper.net/JSA69916	O-JUN-JUNO-071122/5382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages. The evo-aftmand-bt process is asserting. fpc1 evo-aftmand-bt[17556]: %USER-3: get_next_guid: Ran out of Guid Space start 1748051689472 end 1752346656767 fpc1 audit[17556]: %AUTH-5: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 kernel: %KERN-5: audit: type=1701 audit(1648567505.119:57): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=17556 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=6 fpc1 emfd-fpa[14438]: %USER-5: Alarm set: APP color=red, class=CHASSIS, reason=Application evo-aftmand-bt fail on node Fpc1 fpc1 emfd-fpa[14438]: %USER-3-EMF_FPA_ALARM_REP: RaiseAlarm: Alarm(Location: /Chassis[0]/Fpc[1] Module: sysman Object: evo-aftmand-bt:0 Error: 2) reported fpc1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sysepochman[12738]: %USER-5-SYSTEM_REBOOT_EVENT: Reboot [node] [ungraceful reboot] [evo-aftmand-bt exited] The FPC resources can be monitored using the following commands: user@router> start shell [vrf:none] user@router-re0:~$ cli -c "show platform application-info allocations app evo-aftmand-bt" | grep ^fpc | grep -v Route | grep -i -v Nexthop | awk '{total[$1] += $5} END { for (key in total) { print key " " total[key]/4294967296 }}' Once the FPCs become unreachable they must be manually restarted as they do not self-recover. This issue affects Juniper Networks Junos OS Evolved on PTX Series: All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO version 21.2R1-EVO and later versions; 21.3-EVO versions prior to 21.3R3-EVO; 21.4-EVO versions prior to 21.4R2-EVO; 22.1-EVO versions prior to 22.1R2-EVO. **CVE ID : CVE-2022-22211**		
N/A	18-Oct-2022	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability	https://kb.juniper.net/JSA69874	O-JUN-JUNO-071122/5383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the processing of a malformed OSPF TLV in Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause the periodic packet management daemon (PPMD) process to go into an infinite loop, which in turn can cause protocols and functions reliant on PPMD such as OSPF neighbor reachability to be impacted, resulting in a sustained Denial of Service (DoS) condition. The DoS condition persists until the PPMD process is manually restarted. This issue affects: Juniper Networks Junos OS: All versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S9; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S3-EVO; 21.1 versions prior to 21.1R2-EVO.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22224		
N/A	18-Oct-2022	6.5	An Improper Control of a Resource Through its Lifetime vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows unauthenticated adjacent attacker to cause a Denial of Service (DoS). In an EVPN-MPLS scenario, if MAC is learned locally on an access interface but later a request to delete is received indicating that the MAC was learnt remotely, this can lead to memory corruption which can result in line card crash and reload. This issue affects: Juniper Networks Junos OS All versions 17.3R1 and later versions prior to 19.2R3-S5; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S8; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved All versions	https://kb.juniper.net/JSA69907	O-JUN-JUNO-071122/5384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO; 21.4-EVO versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. **CVE ID : CVE-2022-22250**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS, Junos OS Evolved allows a network-based unauthenticated attacker to cause a Denial of Service (DoS). When a BGP flow route with redirect IP extended community is received, and the reachability to the next-hop of the corresponding redirect IP is flapping, the rpd process might crash. Whether the crash occurs depends on the timing of the internally processing of these two events and is outside the attackers control. Please note that this issue also affects Route-Reflectors unless 'routing-options	https://kb.juniper.net/JSA69902	O-JUN-JUNO-071122/5385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flow firewall-install-disable' is configured. This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.4 versions prior to 19.4R3-S8; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22220**		
Time-of-check Time-of-use (TOCTOU) Race Condition	18-Oct-2022	5.9	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated attacker with an established BGP session to cause a Denial of Service (DoS). In a BGP multipath scenario, when one of the contributing routes is flapping often and rapidly, rpd may	https://kb.juniper.net/JSA69875	O-JUN-JUNO-071122/5386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash. As this crash depends on whether a route is a contributing route, and on the internal timing of the events triggered by the flap this vulnerability is outside the direct control of a potential attacker. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S6; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R2-EVO; 21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions 19.2 versions prior to 19.2R2, 19.3R1 and above prior to 20.2R1. Juniper Networks Junos OS Evolved versions prior to 20.2R1-EVO. **CVE ID : CVE-2022-22225**		
Missing Release of Memory	18-Oct-2022	5.5	An Allocation of Resources Without Limits or Throttling and	https://kb.juniper.net/JSA69896	O-JUN-JUNO-071122/5387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
after Effective Lifetime			a Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated low privileged attacker to cause a Denial of Sevice (DoS). In a high-scaled BGP routing environment with rib-sharding enabled, two issues may occur when executing a specific CLI command. One is a memory leak issue with rpd where the leak rate is not constant, and the other is a temporary spike in rpd memory usage during command execution. This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S1-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R1-S2-EVO, 21.2R3-EVO;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.3-EVO versions prior to 21.3R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. **CVE ID : CVE-2022-22240**		
Vendor: lannerinc					
Product: iac-ast2500a_firmware					
Affected Version(s): 1.10.0					
Insufficient Session Expiration	24-Oct-2022	9.8	Session fixation and insufficient session expiration vulnerabilities allow an attacker to perfom session hijacking attacks against users. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-46279**	N/A	O-LAN-IAC--071122/5388
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Oct-2022	9.8	Command injection and multiple stack-based buffer overflows vulnerabilities in the modifyUserb_func function of spx_restservice allow an attacker to execute arbitrary code with the same privileges as the server user (root). This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-26731**	N/A	O-LAN-IAC--071122/5389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-Oct-2022	9.8	A stack-based buffer overflow vulnerability in a subfunction of the Login_handler_func function of spx_restservice allows an attacker to execute arbitrary code with the same privileges as the server user (root). This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-26730**	N/A	O-LAN-IAC--071122/5390
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Oct-2022	9.8	Command injection and multiple stack-based buffer overflows vulnerabilities in the Login_handler_func function of spx_restservice allow an attacker to execute arbitrary code with the same privileges as the server user (root). This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-26729**	N/A	O-LAN-IAC--071122/5391
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Oct-2022	9.8	Command injection and stack-based buffer overflow vulnerabilities in the KillDupUsr_func function of spx_restservice allow an attacker to execute arbitrary code with the same privileges as the server user (root). This issue affects: Lanner Inc	N/A	O-LAN-IAC--071122/5392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-26728**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Oct-2022	9.8	Multiple command injections and stack-based buffer overflows vulnerabilities in the SubNet_handler_func function of spx_restservice allow an attacker to execute arbitrary code with the same privileges as the server user (root). This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-26727**	N/A	O-LAN-IAC--071122/5393
Improper Input Validation	24-Oct-2022	7.5	An improper input validation vulnerability in the TLS certificate generation function allows an attacker to cause a Denial-of-Service (DoS) condition which can only be reverted via a factory reset. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-44769**	N/A	O-LAN-IAC--071122/5394
N/A	24-Oct-2022	7.5	A broken access control vulnerability in the KillDupUsr_func function of spx_restservice allows an attacker to arbitrarily terminate active sessions of other users, causing a Denial-of-Service (DoS)	N/A	O-LAN-IAC--071122/5395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-44467**		
Missing Authorization	24-Oct-2022	7.5	A broken access control vulnerability in the FirstReset_handler_func function of spx_restservice allows an attacker to arbitrarily send reboot commands to the BMC, causing a Denial-of-Service (DoS) condition. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-26733**	N/A	O-LAN-IAC--071122/5396
Observable Discrepancy	24-Oct-2022	5.3	Observable discrepancies in the login process allow an attacker to guess legitimate user names registered in the BMC. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-45925**	N/A	O-LAN-IAC--071122/5397
Missing Authorization	24-Oct-2022	5.3	A broken access control vulnerability in the SubNet_handler_func function of spx_restservice allows an attacker to arbitrarily change the security access rights to KVM and Virtual Media functionalities. This issue	N/A	O-LAN-IAC--071122/5398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-44776**		
Missing Authorization	24-Oct-2022	5.3	A broken access control vulnerability in the First_network_func function of spx_restservice allows an attacker to arbitrarily change the network configuration of the BMC. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0. **CVE ID : CVE-2021-26732**	N/A	O-LAN-IAC--071122/5399
Product: iac-ast2500_firmware					
Affected Version(s): 1.00.0					
Use of Hard-coded Credentials	24-Oct-2022	8.1	Use of hard-coded TLS certificate by default allows an attacker to perform Man-in-the-Middle (MitM) attacks even in the presence of the HTTPS connection. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.00.0. **CVE ID : CVE-2021-4228**	N/A	O-LAN-IAC--071122/5400
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Improper Limitation of a	17-Oct-2022	9.8	This vulnerability could allow a remote attacker to execute remote	N/A	O-LIN-LINU-071122/5401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			commands with improper validation of parameters of certain API constructors. Remote attackers could use this vulnerability to execute malicious commands such as directory traversal. **CVE ID : CVE-2022-23770**		
Use After Free	21-Oct-2022	9.8	A vulnerability was found in Linux Kernel. It has been classified as problematic. Affected is the function nilfs_new_inode of the file fs/nilfs2/inode.c of the component BPF. The manipulation leads to use after free. It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211992. **CVE ID : CVE-2022-3649**	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf-next.git/commit/?id=d325dc6eb763c10f591c239550b8c7e5466a5d09	O-LIN-LINU-071122/5402
Use After Free	21-Oct-2022	8.8	A vulnerability, which was classified as critical, was found in Linux Kernel. Affected is the function l2cap_conn_del of the file net/bluetooth/l2cap_core.c of the component Bluetooth. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue.	https://git.kernel.org/pub/scm/linux/kernel/git/bluetooth/bluetooth-next.git/commit/?id=42cf46dea905a80f6de218e837ba4d4cc33d6979	O-LIN-LINU-071122/5403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The identifier of this vulnerability is VDB-211944. **CVE ID : CVE-2022-3640**		
Use After Free	17-Oct-2022	8	A vulnerability classified as critical has been found in Linux Kernel. Affected is the function btf_dump_name_dups of the file tools/lib/bpf/btf_dump.c of the component libbpf. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211032. **CVE ID : CVE-2022-3534**	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf-next.git/commit/?id=93c660ca40b5d2f7c1b1626e955a8e9fa30e0749	O-LIN-LINU-071122/5404
Use After Free	17-Oct-2022	8	A vulnerability classified as critical was found in Linux Kernel. Affected by this vulnerability is the function l2cap_reassemble_sdu of the file net/bluetooth/l2cap_core.c of the component Bluetooth. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211087. **CVE ID : CVE-2022-3564**	https://git.kernel.org/pub/scm/linux/kernel/git/bluetooth/bluetooth-next.git/commit/?id=89f9f3cb86b1c63badaf392a83dd661d56cc50b1	O-LIN-LINU-071122/5405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Oct-2022	8	A vulnerability, which was classified as critical, has been found in Linux Kernel. Affected by this issue is the function del_timer of the file drivers/isdn/mISDN/l1oip_core.c of the component Bluetooth. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211088. **CVE ID : CVE-2022-3565**	https://git.kernel.org/pub/scm/linux/kernel/git/bluetooth/bluetooth-next.git/commit/?id=2568a7e0832ee30b0a351016d03062ab4e0e0a3f	O-LIN-LINU-071122/5406
Use After Free	21-Oct-2022	7.8	A vulnerability was found in Linux Kernel. It has been classified as critical. This affects the function devlink_param_set/devlink_param_get of the file net/core/devlink.c of the component IPsec. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier VDB-211929 was assigned to this vulnerability. **CVE ID : CVE-2022-3625**	https://git.kernel.org/pub/scm/linux/kernel/git/klassert/ipsec-next.git/commit/?id=6b4db2e528f650c7fb712961aac36455468d5902	O-LIN-LINU-071122/5407
Use After Free	21-Oct-2022	7.8	A vulnerability, which was classified as critical, was found in Linux Kernel. This affects the function __mtk_ppe_check_skb of the file	https://git.kernel.org/pub/scm/linux/kernel/git/pabeni/net-next.git/commit/?id=17a	O-LIN-LINU-071122/5408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drivers/net/ethernet/mediatek/mtk_ppe.c of the component Ethernet Handler. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211935. **CVE ID : CVE-2022-3636**	5f6a78dc7b8db385de346092d7d9f9dc24df6	
Missing Release of Memory after Effective Lifetime	16-Oct-2022	7.5	A vulnerability classified as problematic was found in Linux Kernel. This vulnerability affects the function macvlan_handle_frame of the file drivers/net/macvlan.c of the component skb. The manipulation leads to memory leak. The attack can be initiated remotely. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211024. **CVE ID : CVE-2022-3526**	https://git.kernel.org/pub/scm/linux/kernel/git/pabeni/net-next.git/commit/?id=e16b859872b87650bb55b12cca5a5fcdc49c1442	O-LIN-LINU-071122/5409
NULL Pointer Dereference	20-Oct-2022	7.5	A vulnerability was found in Linux Kernel. It has been classified as problematic. Affected is the function nilfs_bmap_lookup_at_level of the file fs/nilfs2/inode.c of the component nilfs2. The manipulation leads to null pointer dereference.	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf-next.git/commit/?id=21a87d88c2253350e115029	O-LIN-LINU-071122/5410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211920. **CVE ID : CVE-2022-3621**	f14fe2a10a7e6c856	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	20-Oct-2022	7.5	A vulnerability was found in Linux Kernel. It has been declared as problematic. Affected by this vulnerability is the function follow_page_pte of the file mm/gup.c of the component BPF. The manipulation leads to race condition. The attack can be launched remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-211921 was assigned to this vulnerability. **CVE ID : CVE-2022-3623**	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf-next.git/commit/?id=fac35ba763ed07ba93154c95ffc0c4a55023707f	O-LIN-LINU-071122/5411
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Oct-2022	7.1	A vulnerability, which was classified as problematic, was found in Linux Kernel. This affects the function tcp_getsockopt/tcp_setsockopt of the component TCP Handler. The manipulation leads to race condition. It is recommended to apply a patch to fix this issue. The identifier VDB-	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=f49cd2f4d6170d27a2c61f1fecb03d8a70c91f57	O-LIN-LINU-071122/5412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			211089 was assigned to this vulnerability. **CVE ID : CVE-2022-3566**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Oct-2022	7.1	A vulnerability has been found in Linux Kernel and classified as problematic. This vulnerability affects the function inet6_stream_ops/inet6_dgram_ops of the component IPv6 Handler. The manipulation leads to race condition. It is recommended to apply a patch to fix this issue. VDB-211090 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3567**	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=364f997b5cfe1db0d63a390fe7c801fa2b3115f6	O-LIN-LINU-071122/5413
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Oct-2022	7	A vulnerability was found in Linux Kernel and classified as problematic. This issue affects the function hugetlb_no_page of the file mm/hugetlb.c. The manipulation leads to race condition. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211019. **CVE ID : CVE-2022-3522**	https://vuldb.com/?id.211019	O-LIN-LINU-071122/5414
Use After Free	21-Oct-2022	7	A vulnerability, which was classified as critical, has been found in Linux Kernel. Affected by this	https://git.kernel.org/pub/scm/linux/kernel/git/	O-LIN-LINU-071122/5415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is the function tst_timer of the file drivers/atm/idt77252.c of the component IPsec. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. VDB-211934 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3635**	klassert/ipsec-next.git/commit/?id=3f4093e2bf4673f218c0bf17d8362337c400e77b	
Improper Resource Shutdown or Release	17-Oct-2022	5.7	A vulnerability was found in Linux Kernel. It has been classified as problematic. This affects the function get_syms of the file tools/testing/selftests/bpf/prog_tests/kprobe_multi_test.c of the component BPF. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The identifier VDB-211029 was assigned to this vulnerability. **CVE ID : CVE-2022-3531**	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf-next.git/commit/?id=6d2e21dc4db3933db65293552ecc1ede26febeca	O-LIN-LINU-071122/5416
Improper Resource Shutdown or Release	17-Oct-2022	5.7	A vulnerability was found in Linux Kernel. It has been declared as problematic. This vulnerability affects the function test_map_kptr_success/test_fentry of the component BPF. The manipulation leads to memory leak. It is	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf-next.git/commit/?id=6e8280b958c5d7edc514cf34	O-LIN-LINU-071122/5417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recommended to apply a patch to fix this issue. VDB-211030 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3532**	7a800b23b7732b2b	
Improper Resource Shutdown or Release	17-Oct-2022	5.7	A vulnerability was found in Linux Kernel. It has been rated as problematic. This issue affects the function parse_usdt_arg of the file tools/lib/bpf/usdt.c of the component BPF. The manipulation of the argument reg_name leads to memory leak. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211031. **CVE ID : CVE-2022-3533**	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf-next.git/commit/?id=0dc9254e03704c75f2ebc9cbef2ce4de83fba603	O-LIN-LINU-071122/5418
NULL Pointer Dereference	17-Oct-2022	5.7	A vulnerability classified as problematic has been found in Linux Kernel. Affected is the function read_50_controller_cap_complete of the file tools/mgmt-tester.c of the component BlueZ. The manipulation of the argument cap_len leads to null pointer dereference. It is recommended to apply a patch to fix this issue. VDB-211086 is the identifier assigned to this vulnerability.	https://git.kernel.org/pub/scm/bluetooth/bluez.git/commit/?id=e3c92f1f786f0b55440bd908b55894d0c792cf0e	O-LIN-LINU-071122/5419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3563		
NULL Pointer Dereference	19-Oct-2022	5.5	A vulnerability was found in Linux Kernel. It has been classified as problematic. This affects the function find_prog_by_sec_insn of the file tools/lib/bpf/libbpf.c of the component BPF. The manipulation leads to null pointer dereference. It is recommended to apply a patch to fix this issue. The identifier VDB-211749 was assigned to this vulnerability. **CVE ID : CVE-2022-3606**	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf-next.git/commit/?id=d0d382f95a9270dcf803539d6781d6bd67e3f5b2	O-LIN-LINU-071122/5420
Missing Release of Memory after Effective Lifetime	21-Oct-2022	5.5	A vulnerability was found in Linux Kernel. It has been rated as problematic. This issue affects some unknown processing of the file fs/fscache/cookie.c of the component IPsec. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211931. **CVE ID : CVE-2022-3630**	https://git.kernel.org/pub/scm/linux/kernel/git/klassert/ipsec-next.git/commit/?id=fb24771faf72a2fd62b3b6287af3c610c3ec9cf1	O-LIN-LINU-071122/5421
Improper Resource Shutdown or Release	21-Oct-2022	5.5	A vulnerability has been found in Linux Kernel and classified as problematic. This vulnerability affects the	https://git.kernel.org/pub/scm/bluetooth/bluez.git/commit/?i	O-LIN-LINU-071122/5422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function jlink_init of the file monitor/jlink.c of the component BlueZ. The manipulation leads to denial of service. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211936. **CVE ID : CVE-2022-3637**	d=1d6cfb8e625a944010956714c1802bc1e1fc6c4f	
Use of Uninitialized Resource	21-Oct-2022	5.5	A vulnerability classified as problematic has been found in Linux Kernel. This affects the function rtl8188f_spur_calibration of the file drivers/net/wireless/realtek/rtl8xxxu/rtl8xxxu_8188f.c of the component Wireless. The manipulation of the argument hw_ctrl_s1/sw_ctrl_s1 leads to use of uninitialized variable. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211959. **CVE ID : CVE-2022-3642**	https://git.kernel.org/pub/scm/linux/kernel/git/wireless/wireless-next.git/commit/?id=80e5acb6dd72b25a6e6527443b9e9c1c3a7bcef6	O-LIN-LINU-071122/5423
Use After Free	16-Oct-2022	5.3	A vulnerability was found in Linux Kernel. It has been classified as problematic. Affected is an unknown function of the file mm/memory.c of the component Driver Handler. The manipulation leads to	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=16ce101db85db694a91380aa4	O-LIN-LINU-071122/5424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use after free. It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211020. **CVE ID : CVE-2022-3523**	c89b25530871d33	
Missing Release of Memory after Effective Lifetime	21-Oct-2022	5.3	A vulnerability, which was classified as problematic, has been found in Linux Kernel. This issue affects the function nilfs_attach_log_writer of the file fs/nilfs2/segment.c of the component BPF. The manipulation leads to memory leak. The attack may be initiated remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-211961 was assigned to this vulnerability. **CVE ID : CVE-2022-3646**	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf-next.git/commit/?id=d0d51a97063db4704a5ef6bc978dddab1636a306	O-LIN-LINU-071122/5425
Missing Release of Memory after Effective Lifetime	20-Oct-2022	4.3	A vulnerability has been found in Linux Kernel and classified as problematic. This vulnerability affects the function l2cap_recv_acldata of the file net/bluetooth/l2cap_core.c of the component Bluetooth. The manipulation leads to	https://git.kernel.org/pub/scm/linux/kernel/git/bluetooth/bluetooth-next.git/commit/?id=97097c85c088e11651146da	O-LIN-LINU-071122/5426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory leak. It is recommended to apply a patch to fix this issue. VDB-211918 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3619**	32a4e1cdb9dfa6193	
Improper Resource Shutdown or Release	17-Oct-2022	3.5	A vulnerability classified as problematic was found in Linux Kernel. Affected by this vulnerability is the function mvpp2_dbgfs_port_init of the file drivers/net/ethernet/marvell/mvpp2/mvpp2_debugfs.c of the component mvpp2. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The identifier VDB-211033 was assigned to this vulnerability. **CVE ID : CVE-2022-3535**	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf-next.git/commit/?id=0152dfee235e87660f52a117fc9f70dc55956bb4	O-LIN-LINU-071122/5427
Missing Release of Memory after Effective Lifetime	21-Oct-2022	3.3	A vulnerability was found in Linux Kernel and classified as problematic. Affected by this issue is the function rlb_arp_xmit of the file drivers/net/bonding/bond_alb.c of the component IPsec. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The identifier of this	https://git.kernel.org/pub/scm/linux/kernel/git/klassert/ipsec-next.git/commit/?id=4f5d33f4f798b1c6d92b613f0087f639d9836971	O-LIN-LINU-071122/5428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-211928. **CVE ID : CVE-2022-3624**		
Missing Release of Memory after Effective Lifetime	21-Oct-2022	3.3	A vulnerability was found in Linux Kernel. It has been declared as problematic. This vulnerability affects the function vsock_connect of the file net/vmw_vsock/af_vsock.c of the component IPsec. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. VDB-211930 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3629**	https://git.kernel.org/pub/scm/linux/kernel/git/klassert/ipsec-next.git/commit/?id=7e97cfed9929eaabc41829c395eb0d1350fccb9d	O-LIN-LINU-071122/5429
Missing Release of Memory after Effective Lifetime	21-Oct-2022	3.3	A vulnerability classified as problematic has been found in Linux Kernel. Affected is the function j1939_session_destroy of the file net/can/j1939/transport.c of the component IPsec. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211932. **CVE ID : CVE-2022-3633**	https://git.kernel.org/pub/scm/linux/kernel/git/klassert/ipsec-next.git/commit/?id=8c21c54a53ab21842f5050fa090f26b03c0313d6	O-LIN-LINU-071122/5430
Affected Version(s): * Up to (excluding) 2.6.12					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Oct-2022	7.5	A vulnerability was found in Linux Kernel. It has been declared as problematic. Affected by this vulnerability is the function ipv6_renew_options of the component IPv6 Handler. The manipulation leads to memory leak. The attack can be launched remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-211021 was assigned to this vulnerability. **CVE ID : CVE-2022-3524**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3c52c6bb831f6335c176a0fc7214e26f43adbd11	O-LIN-LINU-071122/5431
Affected Version(s): * Up to (excluding) 5.19					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Oct-2022	2.5	A vulnerability has been found in Linux Kernel and classified as problematic. This vulnerability affects the function kcm_tx_work of the file net/kcm/kcmsock.c of the component kcm. The manipulation leads to race condition. It is recommended to apply a patch to fix this issue. VDB-211018 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3521**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ec7eede369fe5b0d085ac51fdbb95184f87bfc6c	O-LIN-LINU-071122/5432
Affected Version(s): * Up to (excluding) 5.19.15					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	26-Oct-2022	7.8	drivers/usb/mon/mon_bin.c in usbmon in the Linux kernel before 5.19.15 and 6.x before 6.0.1 allows a user-space client to corrupt the monitor's internal memory. **CVE ID : CVE-2022-43750**	https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.0.1, https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=a659daf63d16aa883be42f3f34ff84235c302198, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.19.15	O-LIN-LINU-071122/5433
Affected Version(s): * Up to (excluding) 6.0					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Oct-2022	7.8	A vulnerability has been found in Linux Kernel and classified as critical. Affected by this vulnerability is the function area_cache_get of the file drivers/net/ethernet/netronome/nfp/nfpcore/nfp_cppcore.c of the component IPsec. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier VDB-211045 was assigned to this vulnerability. **CVE ID : CVE-2022-3545**	https://git.kernel.org/pub/scm/linux/kernel/git/klassert/ipsec-next.git/commit/?id=02e1a114fdb71e59ee6770294166c30d437bf86a	O-LIN-LINU-071122/5434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	17-Oct-2022	5.5	A vulnerability, which was classified as problematic, was found in Linux Kernel. Affected is the function damon_sysfs_add_target of the file mm/damon/sysfs.c of the component Netfilter. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211044. **CVE ID : CVE-2022-3544**	https://git.kernel.org/pub/scm/linux/kernel/git/netfilter/nf-next.git/commit/?id=1c8e2349f2d033f634d046063b704b2ca6c46972	O-LIN-LINU-071122/5435
Use After Free	19-Oct-2022	5.5	A flaw was found in the Linux kernel's networking code. A use-after-free was found in the way the sch_sfb enqueue function used the socket buffer (SKB) cb field after the same SKB had been enqueued (and freed) into a child qdisc. This flaw allows a local, unprivileged user to crash the system, causing a denial of service. **CVE ID : CVE-2022-3586**	https://github.com/torvalds/linux/commit/9efd23297cca	O-LIN-LINU-071122/5436
Affected Version(s): * Up to (excluding) 6.1					
Improper Restriction of Operations within the	17-Oct-2022	7.8	A vulnerability classified as critical has been found in Linux Kernel. This affects the function spl2sw_nvmem_get_mac_address of the file	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf-next.git/com	O-LIN-LINU-071122/5437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			drivers/net/ethernet/sunplus/spl2sw_driver.c of the component BPF. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier VDB-211041 was assigned to this vulnerability. **CVE ID : CVE-2022-3541**	mit/?id=12aece8b01507a2d357a1861f470e83621fbb6f2	
N/A	18-Oct-2022	7.5	A vulnerability was found in Linux Kernel. It has been declared as problematic. Affected by this vulnerability is the function intr_callback of the file drivers/net/usb/r8152.c of the component BPF. The manipulation leads to logging of excessive data. The attack can be launched remotely. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211363. **CVE ID : CVE-2022-3594**	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf-next.git/commit/?id=93e2be344a7db169b7119de21ac1bf253b8c6907	O-LIN-LINU-071122/5438
Improper Resource Shutdown or Release	17-Oct-2022	5.5	A vulnerability classified as problematic was found in Linux Kernel. This vulnerability affects the function bnx2x_tpa_stop of the file drivers/net/ethernet/broadcom/bnx2x/bnx2x_cmn.c of the component BPF. The manipulation leads to memory leak. It	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf-next.git/commit/?id=b43f9acbb8942b05252be83	O-LIN-LINU-071122/5439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is recommended to apply a patch to fix this issue. VDB-211042 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3542**	ac25a81cec70cc192	
Improper Resource Shutdown or Release	17-Oct-2022	5.5	A vulnerability, which was classified as problematic, has been found in Linux Kernel. This issue affects the function unix_sock_destructor/unix_release_sock of the file net/unix/af_unix.c of the component BPF. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211043. **CVE ID : CVE-2022-3543**	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf-next.git/commit/?id=7a62ed61367b8fd01bae1e18e30602c25060d824	O-LIN-LINU-071122/5440
Double Free	18-Oct-2022	5.5	A vulnerability was found in Linux Kernel. It has been rated as problematic. Affected by this issue is the function sess_free_buffer of the file fs/cifs/sess.c of the component CIFS Handler. The manipulation leads to double free. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211364.	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=b854b4ee66437e6e1622fda90529c814978cb4ca	O-LIN-LINU-071122/5441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3595		
Affected Version(s): * Up to (including) 6.0.3					
Expected Behavior Violation	25-Oct-2022	5.5	A flaw was found in the KVM's AMD nested virtualization (SVM). A malicious L1 guest could purposely fail to intercept the shutdown of a cooperative nested guest (L2), possibly leading to a page fault and kernel panic in the host (L0). **CVE ID : CVE-2022-3344**	https://lore.kernel.org/lkml/20221020093055.224317-5-mlevitsk@redhat.com/T/, https://bugzilla.redhat.com/show_bug.cgi?id=2130278	O-LIN-LINU-071122/5442
Affected Version(s): 2.6.12					
Missing Release of Memory after Effective Lifetime	16-Oct-2022	7.5	A vulnerability was found in Linux Kernel. It has been declared as problematic. Affected by this vulnerability is the function ipv6_renew_options of the component IPv6 Handler. The manipulation leads to memory leak. The attack can be launched remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-211021 was assigned to this vulnerability. **CVE ID : CVE-2022-3524**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3c52c6bb831f6335c176a0fc7214e26f43adbd11	O-LIN-LINU-071122/5443
Affected Version(s): 5.19					
Out-of-bounds Write	20-Oct-2022	7.8	An out-of-bounds memory write flaw was found in the Linux	https://git.kernel.org/pub/scm/linux	O-LIN-LINU-071122/5444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel's Kid-friendly Wired Controller driver. This flaw allows a local user to crash or potentially escalate their privileges on the system. It is in bigben_probe of drivers/hid/hid-bigbenff.c. The reason is incorrect assumption - bigben devices all have inputs. However, malicious devices can break this assumption, leaking to out-of-bound write. **CVE ID : CVE-2022-3577**	/kernel/git/torvalds/linux.git/commit/?id=945a9a8e448b65bec055d37eba58f711b39f66f0, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=fc4ef9d5724973193bfa5ebed181dba6de3a56db	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Oct-2022	2.5	A vulnerability has been found in Linux Kernel and classified as problematic. This vulnerability affects the function kcm_tx_work of the file net/kcm/kcmsock.c of the component kcm. The manipulation leads to race condition. It is recommended to apply a patch to fix this issue. VDB-211018 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3521**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ec7eede369fe5b0d085ac51fdbb95184f87bfc6c	O-LIN-LINU-071122/5445
Affected Version(s): 6.0					
Out-of-bounds Write	26-Oct-2022	7.8	drivers/usb/mon/mon_bin.c in usbmon in the Linux kernel before 5.19.15 and 6.x before 6.0.1 allows a user-space	https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-	O-LIN-LINU-071122/5446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			client to corrupt the monitor's internal memory. **CVE ID : CVE-2022-43750**	6.0.1, https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=a659daf63d16aa883be42f3f34ff84235c302198, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.19.15	
Improper Resource Shutdown or Release	17-Oct-2022	5.5	A vulnerability, which was classified as problematic, was found in Linux Kernel. Affected is the function damon_sysfs_add_target of the file mm/damon/sysfs.c of the component Netfilter. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211044. **CVE ID : CVE-2022-3544**	https://git.kernel.org/pub/scm/linux/kernel/git/netfilter/nf-next.git/commit/?id=1c8e2349f2d033f634d046063b704b2ca6c46972	O-LIN-LINU-071122/5447
Use After Free	19-Oct-2022	5.5	A flaw was found in the Linux kernel's networking code. A use-after-free was found in the way the sch_sfb enqueue function used the socket buffer (SKB) cb field after the same	https://github.com/torvalds/linux/commit/9efd23297cca	O-LIN-LINU-071122/5448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SKB had been enqueued (and freed) into a child qdisc. This flaw allows a local, unprivileged user to crash the system, causing a denial of service. **CVE ID : CVE-2022-3586**		
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Improper Authentication	17-Oct-2022	9.8	Remote code execution vulnerability due to insufficient user privilege verification in reverseWall-MDS. Remote attackers can exploit the vulnerability such as stealing account, through remote code execution. **CVE ID : CVE-2022-23769**	N/A	O-MIC-WIND-071122/5449
Improper Control of Generation of Code ('Code Injection')	25-Oct-2022	9.8	Azure CLI is the command-line interface for Microsoft Azure. In versions previous to 2.40.0, Azure CLI contains a vulnerability for potential code injection. Critical scenarios are where a hosting machine runs an Azure CLI command where parameter values have been provided by an external source. The vulnerability is only applicable when the Azure CLI command is run on a Windows	https://github.com/Azure/azure-cli/security/advisories/GHSA-47xc-9rr2-q7p4, https://github.com/Azure/azure-cli/pull/23514, https://github.com/Azure/azure-cli/pull/24015	O-MIC-WIND-071122/5450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			machine and with any version of PowerShell and when the parameter value contains the `&` or `|` symbols. If any of these prerequisites are not met, this vulnerability is not applicable. Users should upgrade to version 2.40.0 or greater to receive a a mitigation for the vulnerability. **CVE ID : CVE-2022-39327**		
Incorrect Permission Assignment for Critical Resource	21-Oct-2022	7.8	The Automox Agent before 40 on Windows incorrectly sets permissions on key files. **CVE ID : CVE-2022-36122**	https://automox.com, https://www.automox.com/security/security-bulletin	O-MIC-WIND-071122/5451
Out-of-bounds Read	25-Oct-2022	7.8	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/illustrator/apsb22-56.html	O-MIC-WIND-071122/5452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38436		
Improper Input Validation	25-Oct-2022	7.8	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38435**	https://helpx.adobe.com/security/products/illustrator/apsb22-56.html	O-MIC-WIND-071122/5453
Vendor: Netapp					
Product: clustered_data_ontap					
Affected Version(s): 9.11.1					
N/A	19-Oct-2022	8.1	Clustered Data ONTAP versions 9.11.1 through 9.11.1P2 with SnapLock configured FlexGroups are susceptible to a vulnerability which could allow an authenticated remote attacker to arbitrarily modify or delete WORM data prior to the end of the retention period. **CVE ID : CVE-2022-23241**	https://security.netapp.com/advisory/ntap-20221017-0001/	O-NET-CLUS-071122/5454
Vendor: Netgear					
Product: r6220_firmware					
Affected Version(s): 1.1.0.114_1.0.1					
Improper Neutraliz	17-Oct-2022	8.8	Netgear R6220 v1.1.0.114_1.0.1 suffers	https://www.netgear.co	O-NET-R622-071122/5455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation of Special Elements used in a Command ('Command Injection')			from Incorrect Access Control, resulting in a command injection vulnerability. **CVE ID : CVE-2022-42221**	m/about/security/	
Vendor: Oracle					
Product: solaris					
Affected Version(s): 11					
N/A	18-Oct-2022	5.5	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-39401**	https://www.oracle.com/security-alerts/cpuoct2022.html	O-ORA-SOLA-071122/5456
N/A	18-Oct-2022	5.5	Vulnerability in the Oracle Solaris product of	https://www.oracle.co	O-ORA-SOLA-071122/5457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Systems (component: Filesystem). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-39417**	m/security-alerts/cpuoct2022.html	
N/A	18-Oct-2022	3.3	Vulnerability in the Oracle Solaris product of Oracle Systems (component: LDoms). The supported version that is affected is 11. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a	https://www.oracle.com/security-alerts/cpuoct2022.html	O-ORA-SOLA-071122/5458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 3.3 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21610**		
Vendor: oringnet					
Product: iap-420\+_firmware					
Affected Version(s): 2.0m					
Hidden Functionality	21-Oct-2022	8.8	On ORing net IAP-420(+) with FW version 2.0m a telnet server is enabled by default and cannot permanently be disabled. You can connect to the device with with hardcoded credentials and get an administrative shell. These credentials are reset to defaults with every reboot. **CVE ID : CVE-2022-3203**	https://mads.uniud.it/2022/09/lord-of-the-orings/	O-ORI-IAP--071122/5459
Product: iap-420_firmware					
Affected Version(s): 2.0m					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Hidden Functionality	21-Oct-2022	8.8	On ORing net IAP-420(+) with FW version 2.0m a telnet server is enabled by default and cannot permanently be disabled. You can connect to the device with with hardcoded credentials and get an administrative shell. These credentials are reset to defaults with every reboot. **CVE ID : CVE-2022-3203**	https://mads.uniud.it/2022/09/lord-of-the-orings/	O-ORI-IAP--071122/5460
Vendor: Qualcomm					
Product: apq8009w_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5461
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5463
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: apq8009_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5465
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5467
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5469
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5471
Product: apq8016_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5473
Product: apq8017_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5475
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5477
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5479
Product: apq8037_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5481
Product: apq8052_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-APQ8-071122/5482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	etins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5483
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5485
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: apq8053_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5487
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5489
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25719		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5491
Product: apq8056_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5492
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-APQ8-071122/5493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5494
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5496
Product: apq8064au_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5498
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5500
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5501
Product: apq8076_firmware					
Affected Version(s): -					
Buffer Copy without	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing	https://www.qualcomm.com/compa	O-QUA-APQ8-071122/5502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	ny/product-security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5503
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-APQ8-071122/5504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5505
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5507
Exposure of Sensitive Information to an	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-APQ8-071122/5508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	r-2022-bulletin	
Product: apq8084_firmware					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5509
Product: apq8092_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-APQ8-071122/5510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	r-2022-bulletin	
Product: apq8094_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5511
Product: apq8096au_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5512
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5513
Improper Validation	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access	https://www.qualcomm.com/compa	O-QUA-APQ8-071122/5514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	ny/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5515
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset	https://www.qualcomm.com/company/product-	O-QUA-APQ8-071122/5516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	security/bulletins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5517
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5519
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-APQ8-071122/5520
Product: aqt1000_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AQT1-071122/5521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AQT1-071122/5522
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AQT1-071122/5523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AQT1-071122/5524
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AQT1-071122/5525
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AQT1-071122/5526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AQT1-071122/5527
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AQT1-071122/5528
Time-of-check Time-of-use	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size	https://www.qualcomm.com/company/product-	O-QUA-AQT1-071122/5529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AQT1-071122/5530
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AQT1-071122/5531
Exposure of Sensitive Information to an	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-AQT1-071122/5532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AQT1-071122/5533
Product: ar6003_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR60-071122/5534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Product: ar8031_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR80-071122/5535
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR80-071122/5536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR80-071122/5537
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR80-071122/5538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR80-071122/5539
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR80-071122/5540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR80-071122/5541
Product: ar8035_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR80-071122/5542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR80-071122/5543
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR80-071122/5544
Release of Invalid	19-Oct-2022	7.8	Memory corruption due to untrusted pointer	https://www.qualcomm	O-QUA-AR80-071122/5545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR80-071122/5546
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR80-071122/5547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR80-071122/5548
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR80-071122/5549
Product: ar9380_firmware					
Affected Version(s): -					
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer	https://www.qualcomm.com/compa	O-QUA-AR93-071122/5550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR93-071122/5551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR93-071122/5552
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-AR93-071122/5553
Product: csr8811_firmware					
Affected Version(s): -					
Integer Overflow	19-Oct-2022	9.8	Memory corruption in WLAN due to integer	https://www.qualcomm	O-QUA-CSR8-071122/5554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSR8-071122/5555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25719		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSR8-071122/5556
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSR8-071122/5557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSR8-071122/5558
Product: csra6620_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRA-071122/5559
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value	https://www.qualcomm.com/compa	O-QUA-CSRA-071122/5560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	ny/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRA-071122/5561
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in	https://www.qualcomm.com/company/product-security/bull	O-QUA-CSRA-071122/5562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRA-071122/5563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRA-071122/5564
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRA-071122/5565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Product: csra6640_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRA-071122/5566
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRA-071122/5567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRA-071122/5568
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRA-071122/5569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRA-071122/5570
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRA-071122/5571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRA-071122/5572
Product: csrb31024_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRB-071122/5573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRB-071122/5574
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRB-071122/5575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRB-071122/5576
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRB-071122/5577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-CSRB-071122/5578
Product: fsm10056_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-FSM1-071122/5579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-FSM1-071122/5580
Product: ipq4018_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ4-071122/5581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ4-071122/5582
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ4-071122/5583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ4-071122/5584
Product: ipq4019_firmware					
Affected Version(s): -					
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ4-071122/5585
Product: ipq4028_firmware					
Affected Version(s): -					
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer	https://www.qualcomm.com/compa	O-QUA-IPQ4-071122/5586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ4-071122/5587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ4-071122/5588
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ4-071122/5589
Product: ipq4029_firmware					
Affected Version(s): -					
Integer Overflow	19-Oct-2022	9.8	Memory corruption in WLAN due to integer	https://www.qualcomm	O-QUA-IPQ4-071122/5590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ4-071122/5591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ4-071122/5592
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ4-071122/5593
Product: ipq5010_firmware					
Affected Version(s): -					
Integer Overflow	19-Oct-2022	9.8	Memory corruption in WLAN due to integer	https://www.qualcomm	O-QUA-IPQ5-071122/5594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ5-071122/5595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25719		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ5-071122/5596
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ5-071122/5597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ5-071122/5598
Product: ipq5018_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ5-071122/5599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ5-071122/5600
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ5-071122/5601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ5-071122/5602
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ5-071122/5603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Product: ipq5028_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ5-071122/5604
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ5-071122/5605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ5-071122/5606
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ5-071122/5607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ5-071122/5608
Product: ipq6000_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ6-071122/5609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ6-071122/5610
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ6-071122/5611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ6-071122/5612
Product: ipq6010_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ6-071122/5613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ6-071122/5614
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ6-071122/5615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ6-071122/5616
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different	https://www.qualcomm.com/company/product-	O-QUA-IPQ6-071122/5617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	security/bulletins/october-2022-bulletin	
Product: ipq6018_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ6-071122/5618
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ6-071122/5619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ6-071122/5620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ6-071122/5621
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ6-071122/5622
Product: ipq6028_firmware					
Affected Version(s): -					
Integer Overflow	19-Oct-2022	9.8	Memory corruption in WLAN due to integer	https://www.qualcomm	O-QUA-IPQ6-071122/5623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ6-071122/5624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25719		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ6-071122/5625
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ6-071122/5626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ6-071122/5627
Product: ipq8064_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5629
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5631
Product: ipq8065_firmware					
Affected Version(s): -					
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5632
Product: ipq8068_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5633
Product: ipq8069_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5635
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Product: ipq8070a_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5637
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5639
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5641
Product: ipq8070_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5643
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5645
Product: ipq8071a_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5647
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5649
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: ipq8071_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5651
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5653
Product: ipq8072a_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5655
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ8-071122/5656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5657
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-071122/5658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	security/bulletins/october-2022-bulletin	
Product: ipq8072_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5659
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ8-071122/5660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5661
Product: ipq8074a_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5662
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5664
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5666
Product: ipq8074_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5668
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: ipq8076a_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5670
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5672
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5674
Product: ipq8076_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5676
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5678
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-IPQ8-071122/5679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Product: ipq8078a_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5680
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5682
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-IPQ8-071122/5683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5684
Product: ipq8078_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5686
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-IPQ8-071122/5687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5688
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ8-071122/5689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	etins/october-2022-bulletin	
Product: ipq8173_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5690
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-IPQ8-071122/5691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5692
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-071122/5693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5694
Product: ipq8174_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-IPQ8-071122/5695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5697
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ8-071122/5699
Product: ipq9008_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ9-071122/5700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ9-071122/5701
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-IPQ9-071122/5702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: kailua_firmware					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-KAIL-071122/5703
Product: mdm8215m_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM8-071122/5704
Product: mdm8215_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value	https://www.qualcomm.com/compa	O-QUA-MDM8-071122/5705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	ny/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM8-071122/5706
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in	https://www.qualcomm.com/company/product-security/bull	O-QUA-MDM8-071122/5707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM8-071122/5708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM8-071122/5709
Product: mdm8615m_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM8-071122/5710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Product: mdm9150_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5711
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5712
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to	https://www.qualcomm.com/compa	O-QUA-MDM9-071122/5713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	ny/product-security/bulletins/october-2022-bulletin	
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5714
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: mdm9205_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5716
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: mdm9206_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5718
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5720
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5722
Product: mdm9215_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5724
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5726
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: mdm9225m_firmware					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5728
Product: mdm9225_firmware					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing	https://www.qualcomm.com/company/product-	O-QUA-MDM9-071122/5729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	security/bulletins/october-2022-bulletin	
Product: mdm9230_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5731
Product: mdm9235m_firmware					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: mdm9250_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5733
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5735
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5737
Product: mdm9310_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5739
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5741
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: mdm9330_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5743
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: mdm9607_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5745
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5747
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5749
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: mdm9615m_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5751
Product: mdm9615_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5753
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5755
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: mdm9625m_firmware					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5757
Product: mdm9625_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5758
Product: mdm9628_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5760
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5762
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5764
Product: mdm9630_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5766
Product: mdm9635m_firmware					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: mdm9640_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5768
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5770
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: mdm9645_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5772
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in	https://www.qualcomm.com/company/product-security/bull	O-QUA-MDM9-071122/5773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5774
Product: mdm9650_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5775
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5776
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-MDM9-071122/5777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5778
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-MDM9-071122/5779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5780
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MDM9-071122/5781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: msm8108_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5782
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5784
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25719		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5786
Product: msm8208_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5787
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-MSM8-071122/5788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5789
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5791
Product: msm8209_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5793
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5795
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: msm8608_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5797
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5798
Improper Validation	19-Oct-2022	9.8	Memory corruption in WLAN due to out of	https://www.qualcomm	O-QUA-MSM8-071122/5799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5800
Exposure of Sensitive	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU	https://www.qualcomm.com/compa	O-QUA-MSM8-071122/5801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information to an Unauthorized Actor			reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	ny/product-security/bulletins/october-2022-bulletin	
Product: msm8909w_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5802
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5804
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: msm8917_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5806
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5808
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: msm8920_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5810
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: msm8937_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5812
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-MSM8-071122/5813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	r-2022-bulletin	
Product: msm8940_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5815
Product: msm8952_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5817
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5819
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5820
Product: msm8953_firmware					
Affected Version(s): -					
Buffer Copy	19-Oct-2022	9.8	memory corruption in video due to buffer	https://www.qualcomm	O-QUA-MSM8-071122/5821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	.com/company/product-security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5822
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-MSM8-071122/5823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5824
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-MSM8-071122/5825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	r-2022-bulletin	
Product: msm8956_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5826
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5828
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5830
Product: msm8976sg_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5831
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication	https://www.qualcomm.com/company/product-	O-QUA-MSM8-071122/5832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5833
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-MSM8-071122/5834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	r-2022-bulletin	
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5835
Product: msm8976_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5837
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5839
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5841
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: msm8992_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5843
Product: msm8994_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Product: msm8996au_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5845
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5847
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5849
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5850
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5852
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-MSM8-071122/5853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25664		
Product: pm8937_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-PM89-071122/5854
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-PM89-071122/5855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: pmp8074_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-PMP8-071122/5856
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-PMP8-071122/5857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-PMP8-071122/5858
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-PMP8-071122/5859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: qam8295p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QAM8-071122/5860
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QAM8-071122/5861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QAM8-071122/5862
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QAM8-071122/5863
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QAM8-071122/5864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	r-2022-bulletin	
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QAM8-071122/5865
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QAM8-071122/5866
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QAM8-071122/5867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QAM8-071122/5868
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QAM8-071122/5869
Time-of-check Time-of-	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of	https://www.qualcomm.com/compa	O-QUA-QAM8-071122/5870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	ny/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QAM8-071122/5871
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QAM8-071122/5872
Product: qca0000_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA0-071122/5873
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA0-071122/5874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Product: qca1023_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA1-071122/5875
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA1-071122/5876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA1-071122/5877
Product: qca1062_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA1-071122/5878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA1-071122/5879
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA1-071122/5880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA1-071122/5881
Product: qca1064_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA1-071122/5882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA1-071122/5883
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA1-071122/5884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA1-071122/5885
Product: qca1990_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA1-071122/5886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA1-071122/5887
Product: qca2062_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5889
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5891
Product: qca2064_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5893
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5895
Product: qca2065_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5897
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5899
Product: qca2066_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5901
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA2-071122/5903
Product: qca4004_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5904
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing	https://www.qualcomm.com/company/product-	O-QUA-QCA4-071122/5905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	security/bulletins/october-2022-bulletin	
Product: qca4010_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5907
Product: qca4020_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25687		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5909
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5911
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5913
Product: qca4024_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5915
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5917
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5919
Product: qca4531_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA4-071122/5921
Product: qca6164_firmware					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/5922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	r-2022-bulletin	
Product: qca6174a_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5923
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/5924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5925
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5927
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/5928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5929
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5930
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-071122/5931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5932
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5934
Product: qca6174_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5936
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5938
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Product: qca6175a_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5940
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5942
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qca6310_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5944
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5946
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5948
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5949
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5951
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5953
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5954
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5956
Product: qca6320_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5957
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/5958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5959
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5961
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5963
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5965
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5966
Product: qca6335_firmware					
Affected Version(s): -					
Buffer Copy without	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing	https://www.qualcomm.com/compa	O-QUA-QCA6-071122/5967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	ny/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5968
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5970
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5971
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5973
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5975
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5976
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5978
Product: qca6390_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5979
Improper Validation	19-Oct-2022	9.8	Memory corruption in WLAN due to out of	https://www.qualcomm	O-QUA-QCA6-071122/5980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	.com/company/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5981
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon	https://www.qualcomm.com/compa	O-QUA-QCA6-071122/5982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	ny/product-security/bulletins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5983
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5984
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5986
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25665		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5988
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5989
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25663		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5991
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5992
Product: qca6391_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/5993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5994
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5996
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5997
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25662		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/5999
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6001
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6002
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6004
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6005
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: qca6420_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6007
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6009
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6010
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25661		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6012
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6014
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6015
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6017
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6018
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: qca6421_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6020
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6022
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6023
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25661		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6025
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6026
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in	https://www.qualcomm.com/company/product-	O-QUA-QCA6-071122/6027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6028
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6030
Product: qca6426_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6031
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/6032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6033
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/6034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6035
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6036
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6038
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6039
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in	https://www.qualcomm	O-QUA-QCA6-071122/6040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	.com/company/product-security/bulletins/october-2022-bulletin	
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6041
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: qca6428_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6043
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6045
Product: qca6430_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6047
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6049
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6050
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6052
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6053
Time-of-check Time-of-use	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size	https://www.qualcomm.com/company/product-	O-QUA-QCA6-071122/6054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6055
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6056
Exposure of Sensitive Information to an	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-071122/6057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6058
Product: qca6431_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6060
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6062
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6063
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6065
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6067
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6068
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22078		
Product: qca6436_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6070
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6071
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer	https://www.qualcomm.com/compa	O-QUA-QCA6-071122/6072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	ny/product-security/bulletins/october-2022-bulletin	
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6073
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6075
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6076
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/6077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6078
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6079
Exposure of	19-Oct-2022	5.5	Information disclosure due to exposure of	https://www.qualcomm	O-QUA-QCA6-071122/6080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information to an Unauthorized Actor			information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	.com/company/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6081
Product: qca6438_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6083
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/6084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Product: qca6554a_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6085
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming	https://www.qualcomm.com/company/product-	O-QUA-QCA6-071122/6086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6087
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-071122/6088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6089
Product: qca6564au_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6090
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6091
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-071122/6092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6093
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/6094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6095
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6096
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6098
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6100
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6101
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6103
Product: qca6564a_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6104
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/6105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6106
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6108
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6109
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/6110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6111
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6113
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6114
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6116
Product: qca6564_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6117
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication	https://www.qualcomm.com/company/product-	O-QUA-QCA6-071122/6118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6119
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/6120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6121
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6123
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6125
Product: qca6574au_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6126
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/6127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6128
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6130
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6131
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/6132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6133
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6135
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6136
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33214		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6138
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6139
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: qca6574a_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6141
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6143
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6145
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6146
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6147
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-071122/6148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6149
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6151
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6152
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6154
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6155
Product: qca6574_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6156
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6157
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-071122/6158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6159
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/6160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6161
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6162
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-071122/6163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6164
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6165
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to	https://www.qualcomm.com/compa	O-QUA-QCA6-071122/6166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	ny/product-security/bulletins/october-2022-bulletin	
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6167
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: qca6584au_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6169
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6171
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6173
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6174
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qca6584_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6176
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming	https://www.qualcomm.com/company/product-	O-QUA-QCA6-071122/6177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6178
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-071122/6179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6180
Product: qca6595au_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6181
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6182
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-071122/6183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6184
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-071122/6185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6186
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6187
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6189
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6191
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6192
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6194
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6195
Product: qca6595_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6197
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6199
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6200
Release of Invalid	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in	https://www.qualcomm.com/compa	O-QUA-QCA6-071122/6201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6202
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6204
Product: qca6694_firmware					
Affected Version(s): -					
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Product: qca6696_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6206
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6208
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6210
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6211
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6212
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6214
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6216
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6217
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6219
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA6-071122/6220
Product: qca7500_firmware					
Affected Version(s): -					
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA7-071122/6221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Product: qca8072_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6222
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA8-071122/6223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6224
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA8-071122/6225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Product: qca8075_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6226
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA8-071122/6227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6228
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA8-071122/6229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	etins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6230
Product: qca8081_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA8-071122/6231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6232
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA8-071122/6233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	r-2022-bulletin	
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6234
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6235
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA8-071122/6236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6237
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA8-071122/6238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	etins/octobe r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://ww w.qualcomm .com/compa ny/product-security/bull etins/octobe r-2022-bulletin	O-QUA-QCA8-071122/6239
Product: qca8082_firmware					
Affected Version(s): -					
Integer Overflow or Wraparou nd	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://ww w.qualcomm .com/compa ny/product-security/bull etins/octobe r-2022-bulletin	O-QUA-QCA8-071122/6240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6241
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qca8084_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6243
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6245
Product: qca8085_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6247
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA8-071122/6248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Product: qca8337_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6249
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA8-071122/6250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	etins/october-2022-bulletin	
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6251
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6252
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens	https://www.qualcomm.com/compa	O-QUA-QCA8-071122/6253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6255
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6256
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6257
Integer Overflow	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a	https://www.qualcomm	O-QUA-QCA8-071122/6258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	.com/company/product-security/bulletins/october-2022-bulletin	
Product: qca8386_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6260
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA8-071122/6261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Product: qca9367_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6262
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6264
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6266
Product: qca9369_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6268
Product: qca9377_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25687		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6270
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6272
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6274
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6275
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6277
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6278
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA9-071122/6279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	etins/october-2022-bulletin	
Product: qca9379_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6280
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6282
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6284
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qca9880_firmware					
Affected Version(s): -					
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6286
Product: qca9886_firmware					
Affected Version(s): -					
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: qca9888_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6288
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6290
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6292
Product: qca9889_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6294
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA9-071122/6295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6296
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA9-071122/6297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Product: qca9898_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6298
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6300
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA9-071122/6301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Product: qca9980_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6302
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6304
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA9-071122/6305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Product: qca9984_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6306
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6308
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA9-071122/6309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Product: qca9985_firmware					
Affected Version(s): -					
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6310
Product: qca9990_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6312
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6314
Product: qca9992_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6316
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6318
Product: qca9994_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6320
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCA9-071122/6322
Product: qcc5100_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCC5-071122/6323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCC5-071122/6324
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCC5-071122/6325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCC5-071122/6326
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCC5-071122/6327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCC5-071122/6328
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCC5-071122/6329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCC5-071122/6330
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCC5-071122/6331
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCC5-071122/6332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: qcm2290_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM2-071122/6333
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM2-071122/6334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM2-071122/6335
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM2-071122/6336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM2-071122/6337
Product: qcm4290_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM4-071122/6338
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCM4-071122/6339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM4-071122/6340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM4-071122/6341
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM4-071122/6342
Product: qcm6125_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCM6-071122/6343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	etins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM6-071122/6344
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM6-071122/6345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM6-071122/6346
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM6-071122/6347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM6-071122/6348
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM6-071122/6349
Product: qcm6490_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM6-071122/6350
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM6-071122/6351
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-QCM6-071122/6352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	security/bulletins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM6-071122/6353
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM6-071122/6354
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while	https://www.qualcomm.com/compa	O-QUA-QCM6-071122/6355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	ny/product-security/bulletins/october-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCM6-071122/6356
Product: qcn5021_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6358
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCN5-071122/6359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6360
Product: qcn5022_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6362
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN5-071122/6363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6364
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different	https://www.qualcomm.com/company/product-	O-QUA-QCN5-071122/6365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	security/bulletins/october-2022-bulletin	
Product: qcn5024_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6366
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN5-071122/6367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6369
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6370
Product: qcn5052_firmware					
Affected Version(s): -					
Integer Overflow	19-Oct-2022	9.8	Memory corruption in WLAN due to integer	https://www.qualcomm	O-QUA-QCN5-071122/6371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25719		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6373
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6375
Product: qcn5054_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6377
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6379
Product: qcn5122_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6381
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6383
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Product: qcn5124_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6385
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6387
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6389
Product: qcn5152_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6391
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6393
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: qcn5154_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6395
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6397
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6399
Product: qcn5164_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6401
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN5-071122/6403
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCN5-071122/6404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Product: qcn6023_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6405
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6407
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCN6-071122/6408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6409
Product: qcn6024_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6411
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6413
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCN6-071122/6414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6415
Product: qcn6100_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6417
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCN6-071122/6418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Product: qcn6102_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6419
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens	https://www.qualcomm.com/compa	O-QUA-QCN6-071122/6420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6421
Product: qcn6112_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6422
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6424
Product: qcn6122_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6426
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6428
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: qcn6132_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6430
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6432
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN6-071122/6434
Product: qcn7605_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN7-071122/6435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN7-071122/6436
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN7-071122/6437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN7-071122/6438
Product: qcn7606_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN7-071122/6439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN7-071122/6440
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN7-071122/6441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN7-071122/6442
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN7-071122/6443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN7-071122/6444
Product: qcn9000_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6446
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6448
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Product: qcn9001_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6450
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6452
Product: qcn9002_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6454
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qcn9003_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6456
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT	https://www.qualcomm.com/company/product-	O-QUA-QCN9-071122/6457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6458
Product: qcn9011_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6459
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6460
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6462
Product: qcn9012_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN9-071122/6463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	etins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6464
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6466
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: qcn9022_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6468
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6470
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6472
Product: qcn9024_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6474
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6476
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6478
Product: qcn9070_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6480
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6482
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Product: qcn9072_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6484
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6486
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6488
Product: qcn9074_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6490
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCN9-071122/6491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6492
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCN9-071122/6493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Product: qcn9100_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6494
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6496
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCN9-071122/6497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6498
Product: qcn9274_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCN9-071122/6500
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCN9-071122/6501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Product: qcs2290_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS2-071122/6502
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS2-071122/6503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS2-071122/6504
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCS2-071122/6505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS2-071122/6506
Product: qcs405_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6508
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6510
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6512
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qcs410_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6514
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6516
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6518
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6520
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6521
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: qcs4290_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6523
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6525
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS4-071122/6527
Product: qcs603_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6529
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6530
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6532
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6533
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCS6-071122/6534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	r-2022-bulletin	
Product: qcs605_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6535
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6537
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6538
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QCS6-071122/6539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6540
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6542
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6543
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: qcs610_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6545
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6547
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6548
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens	https://www.qualcomm.com/compa	O-QUA-QCS6-071122/6549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6551
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6552
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25664		
Product: qcs6125_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6554
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6555
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer	https://www.qualcomm.com/compa	O-QUA-QCS6-071122/6556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6558
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6559
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCS6-071122/6560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	r-2022-bulletin	
Product: qcs6490_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6561
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6563
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6564
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6566
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS6-071122/6567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcs8155_firmware					
Affected Version(s): -					
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS8-071122/6568
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS8-071122/6569
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCS8-071122/6570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: qcx315_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCX3-071122/6571
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCX3-071122/6572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCX3-071122/6573
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QCX3-071122/6574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qet4101_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QET4-071122/6575
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QET4-071122/6576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QET4-071122/6577
Product: qrb5165m_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QRB5-071122/6578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QRB5-071122/6579
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QRB5-071122/6580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QRB5-071122/6581
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QRB5-071122/6582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: qrb5165n_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QRB5-071122/6583
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QRB5-071122/6584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QRB5-071122/6585
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QRB5-071122/6586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QRB5-071122/6587
Product: qrb5165_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QRB5-071122/6588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QRB5-071122/6589
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QRB5-071122/6590
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QRB5-071122/6591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QRB5-071122/6592
Product: qsm8250_firmware					
Affected Version(s): -					
Integer Overflow	19-Oct-2022	9.8	Memory corruption in WLAN due to integer	https://www.qualcomm	O-QUA-QSM8-071122/6593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QSM8-071122/6594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QSM8-071122/6595
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QSM8-071122/6596
Exposure of Sensitive Information to an	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QSM8-071122/6597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	etins/october-2022-bulletin	
Product: qsm8350_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QSM8-071122/6598
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QSM8-071122/6599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QSM8-071122/6600
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QSM8-071122/6601
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QSM8-071122/6602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QSM8-071122/6603
Product: qsw8573_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QSW8-071122/6604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QSW8-071122/6605
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QSW8-071122/6606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: qualcomm215_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QUAL-071122/6607
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QUAL-071122/6608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QUAL-071122/6609
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QUAL-071122/6610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QUAL-071122/6611
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-QUAL-071122/6612
Product: sa4150p_firmware					
Affected Version(s): -					
Buffer Copy without Checking	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-SA41-071122/6613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6614
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6616
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6618
Product: sa4155p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25687		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6620
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6622
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6624
Product: sa415m_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6626
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6628
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA41-071122/6630
Product: sa515m_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA51-071122/6631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA51-071122/6632
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA51-071122/6633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA51-071122/6634
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA51-071122/6635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA51-071122/6636
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA51-071122/6637
Product: sa6145p_firmware					
Affected Version(s): -					
Buffer Copy	19-Oct-2022	9.8	memory corruption in video due to buffer	https://www.qualcomm	O-QUA-SA61-071122/6638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	.com/company/product-security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6639
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SA61-071122/6640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6641
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SA61-071122/6642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6643
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6644
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6646
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6648
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6649
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6651
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6652
Product: sa6150p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6654
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6656
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6657
Release of Invalid	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in	https://www.qualcomm.com/compa	O-QUA-SA61-071122/6658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6659
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6661
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6663
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6664
Product: sa6155p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6666
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6668
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6669
Release of Invalid	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in	https://www.qualcomm.com/compa	O-QUA-SA61-071122/6670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6671
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6672
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6674
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25665		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6676
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6677
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6679
Product: sa6155_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6680
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper	https://www.qualcomm	O-QUA-SA61-071122/6681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	.com/company/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6683
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6684
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6685
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6687
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6689
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6690
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25664		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA61-071122/6692
Product: sa8145p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6693
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA81-071122/6694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	etins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6695
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SA81-071122/6696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	r-2022-bulletin	
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6697
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6699
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6701
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6702
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6704
Product: sa8150p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6705
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper	https://www.qualcomm	O-QUA-SA81-071122/6706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	.com/company/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6707
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing	https://www.qualcomm.com/company/product-	O-QUA-SA81-071122/6708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	security/bulletins/october-2022-bulletin	
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6709
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6711
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6712
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6714
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6715
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SA81-071122/6716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6717
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6718
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA81-071122/6719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	etins/october-2022-bulletin	
Product: sa8155p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6720
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6722
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6724
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6725
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6727
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6728
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SA81-071122/6729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6730
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6731
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA81-071122/6732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	etins/october-2022-bulletin	
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6733
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22078		
Product: sa8155_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6735
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6737
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6739
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6740
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6741
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6743
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6745
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6746
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25664		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6748
Product: sa8195p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6749
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA81-071122/6750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	etins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6751
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SA81-071122/6752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	r-2022-bulletin	
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6753
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6755
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6757
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6758
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA81-071122/6760
Product: sa8295p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA82-071122/6761
Improper Validation	19-Oct-2022	9.8	Memory corruption in WLAN due to out of	https://www.qualcomm	O-QUA-SA82-071122/6762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	.com/company/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA82-071122/6763
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon	https://www.qualcomm.com/compa	O-QUA-SA82-071122/6764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	ny/product-security/bulletins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA82-071122/6765
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA82-071122/6766
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA82-071122/6767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25662		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA82-071122/6768
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA82-071122/6769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA82-071122/6770
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA82-071122/6771
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA82-071122/6772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA82-071122/6773
Product: sa8540p_firmware					
Affected Version(s): -					
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA85-071122/6774
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA85-071122/6775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA85-071122/6776
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA85-071122/6777
Product: sa9000p_firmware					
Affected Version(s): -					
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA90-071122/6778
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA90-071122/6779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25661		
Out-of-bounds Write	19-Oct-2022	7.8	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto **CVE ID : CVE-2022-33210**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA90-071122/6780
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SA90-071122/6781
Product: sc8180x\+sdx55_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SC81-071122/6782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SC81-071122/6783
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SC81-071122/6784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: sd205_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD20-071122/6785
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD20-071122/6786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD20-071122/6787
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD20-071122/6788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD20-071122/6789
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD20-071122/6790
Product: sd210_firmware					
Affected Version(s): -					
Buffer Copy without Checking	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-SD21-071122/6791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD21-071122/6792
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD21-071122/6793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD21-071122/6794
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD21-071122/6795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD21-071122/6796
Product: sd429_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD42-071122/6797
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper	https://www.qualcomm	O-QUA-SD42-071122/6798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	.com/company/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD42-071122/6799
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing	https://www.qualcomm.com/company/product-	O-QUA-SD42-071122/6800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	security/bulletins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD42-071122/6801
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD42-071122/6802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD42-071122/6803
Product: sd439_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD43-071122/6804
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper	https://www.qualcomm	O-QUA-SD43-071122/6805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	.com/company/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD43-071122/6806
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing	https://www.qualcomm.com/company/product-	O-QUA-SD43-071122/6807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	security/bulletins/october-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD43-071122/6808
Product: sd450_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD45-071122/6809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD45-071122/6810
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD45-071122/6811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD45-071122/6812
Product: sd460_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD46-071122/6813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD46-071122/6814
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD46-071122/6815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD46-071122/6816
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD46-071122/6817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD46-071122/6818
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD46-071122/6819
Product: sd480_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD48-071122/6820
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD48-071122/6821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD48-071122/6822
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD48-071122/6823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD48-071122/6824
Product: sd632_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD63-071122/6825
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD63-071122/6826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD63-071122/6827
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD63-071122/6828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: sd660_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6829
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6831
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6833
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6835
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6836
Product: sd662_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6837
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6838
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD66-071122/6839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6840
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD66-071122/6841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6842
Product: sd665_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6844
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD66-071122/6846
Product: sd670_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6848
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6850
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6851
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6853
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6854
Product: sd675_firmware					
Affected Version(s): -					
Buffer Copy without	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing	https://www.qualcomm.com/compa	O-QUA-SD67-071122/6855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	ny/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6856
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6858
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6859
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6861
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD67-071122/6862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25665	r-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6863
Product: sd678_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6864
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6866
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25660		
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6868
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6869
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD67-071122/6870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6871
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD67-071122/6872
Product: sd680_firmware					
Affected Version(s): -					
Buffer Copy	19-Oct-2022	9.8	memory corruption in video due to buffer	https://www.qualcomm	O-QUA-SD68-071122/6873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	.com/company/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD68-071122/6874
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD68-071122/6875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD68-071122/6876
Time-of-check Time-of-use (TOCTOU	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD68-071122/6877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
) Race Condition			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	etins/october-2022-bulletin	
Product: sd690_5g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD69-071122/6878
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD69-071122/6879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD69-071122/6880
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD69-071122/6881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD69-071122/6882
Product: sd695_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD69-071122/6883
Integer Overflow	19-Oct-2022	9.8	Memory corruption in WLAN due to integer	https://www.qualcomm	O-QUA-SD69-071122/6884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD69-071122/6885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD69-071122/6886
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD69-071122/6887
Product: sd710_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD71-071122/6888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	etins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD71-071122/6889
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD71-071122/6890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD71-071122/6891
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD71-071122/6892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD71-071122/6893
Product: sd712_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD71-071122/6894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD71-071122/6895
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD71-071122/6896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: sd720g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD72-071122/6897
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD72-071122/6898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD72-071122/6899
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD72-071122/6900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD72-071122/6901
Product: sd730_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD73-071122/6902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD73-071122/6903
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD73-071122/6904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD73-071122/6905
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD73-071122/6906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD73-071122/6907
Product: sd750g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD75-071122/6908
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD75-071122/6909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD75-071122/6910
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD75-071122/6911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD75-071122/6912
Product: sd765g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6914
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6915
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD76-071122/6916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6917
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6919
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6920
Product: sd765_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6922
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6923
Release of Invalid	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in	https://www.qualcomm.com/compa	O-QUA-SD76-071122/6924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6925
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6927
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6928
Product: sd768g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6930
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6932
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6933
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6935
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD76-071122/6936
Product: sd778g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD77-071122/6937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD77-071122/6938
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD77-071122/6939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25660		
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD77-071122/6940
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD77-071122/6941
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD77-071122/6942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD77-071122/6943
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD77-071122/6944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD77-071122/6945
Product: sd780g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD78-071122/6946
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD78-071122/6947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD78-071122/6948
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD78-071122/6949
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD78-071122/6950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD78-071122/6951
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD78-071122/6952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD78-071122/6953
Product: sd7c_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD7C-071122/6954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD7C-071122/6955
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD7C-071122/6956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD7C-071122/6957
Product: sd820_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD82-071122/6958
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD82-071122/6959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD82-071122/6960
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD82-071122/6961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD82-071122/6962
Exposure of Sensitive Information to an	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD82-071122/6963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	r-2022-bulletin	
Product: sd821_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD82-071122/6964
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD82-071122/6965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD82-071122/6966
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD82-071122/6967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD82-071122/6968
Product: sd835_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD83-071122/6969
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value	https://www.qualcomm.com/compa	O-QUA-SD83-071122/6970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	ny/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD83-071122/6971
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD83-071122/6972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	etins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD83-071122/6973
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD83-071122/6974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD83-071122/6975
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD83-071122/6976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD83-071122/6977
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD83-071122/6978
Product: sd845_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD84-071122/6979
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD84-071122/6980
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD84-071122/6981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	etins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD84-071122/6982
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD84-071122/6983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD84-071122/6984
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD84-071122/6985
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD84-071122/6986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD84-071122/6987
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD84-071122/6988
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in	https://www.qualcomm	O-QUA-SD84-071122/6989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	.com/company/product-security/bulletins/october-2022-bulletin	
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD84-071122/6990
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD84-071122/6991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: sd850_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/6992
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/6993
Release of Invalid	19-Oct-2022	7.8	Memory corruption due to untrusted pointer	https://www.qualcomm	O-QUA-SD85-071122/6994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/6995
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/6996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/6997
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/6998
Product: sd855_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/6999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/7000
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/7001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/7002
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/7003
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/7004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/7005
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/7006
Time-of-check Time-of-	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of	https://www.qualcomm.com/compa	O-QUA-SD85-071122/7007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	ny/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/7008
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/7009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD85-071122/7010
Product: sd865_5g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD86-071122/7011
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD86-071122/7012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD86-071122/7013
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD86-071122/7014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD86-071122/7015
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD86-071122/7016
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD86-071122/7017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD86-071122/7018
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD86-071122/7019
Time-of-check	19-Oct-2022	7	Memory corruption in display due to time-of-	https://www.qualcomm	O-QUA-SD86-071122/7020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	.com/company/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD86-071122/7021
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD86-071122/7022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD86-071122/7023
Product: sd870_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD87-071122/7024
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD87-071122/7025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	r-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD87-071122/7026
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD87-071122/7027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD87-071122/7028
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD87-071122/7029
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD87-071122/7030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD87-071122/7031
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD87-071122/7032
Time-of-check	19-Oct-2022	7	Memory corruption in display due to time-of-	https://www.qualcomm	O-QUA-SD87-071122/7033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	.com/company/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD87-071122/7034
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD87-071122/7035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD87-071122/7036
Product: sd888_5g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD88-071122/7037
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD88-071122/7038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	r-2022-bulletin	
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD88-071122/7039
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD88-071122/7040
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD88-071122/7041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD88-071122/7042
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD88-071122/7043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD88-071122/7044
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD88-071122/7045
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD88-071122/7046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD88-071122/7047
Product: sd888_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD88-071122/7048
Integer Overflow	19-Oct-2022	9.8	Memory corruption in WLAN due to integer	https://www.qualcomm	O-QUA-SD88-071122/7049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	.com/company/product-security/bulletins/october-2022-bulletin	
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD88-071122/7050
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD88-071122/7051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD88-071122/7052
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD88-071122/7053
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD88-071122/7054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD88-071122/7055
Product: sda429w_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDA4-071122/7056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDA4-071122/7057
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDA4-071122/7058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDA4-071122/7059
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDA4-071122/7060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDA4-071122/7061
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDA4-071122/7062
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDA4-071122/7063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25664		
Product: sdm429w_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDM4-071122/7064
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDM4-071122/7065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDM4-071122/7066
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDM4-071122/7067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDM4-071122/7068
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDM4-071122/7069
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDM4-071122/7070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: sdm630_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDM6-071122/7071
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDM6-071122/7072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDM6-071122/7073
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDM6-071122/7074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: sdw2500_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDW2-071122/7075
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDW2-071122/7076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDW2-071122/7077
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDW2-071122/7078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: sdx12_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX1-071122/7079
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX1-071122/7080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX1-071122/7081
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX1-071122/7082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: sdx20m_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7083
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7085
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7087
Product: sdx20_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7089
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7091
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Product: sdx24_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7093
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7095
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7096
Release of Invalid	19-Oct-2022	7.8	Memory corruption due to untrusted pointer	https://www.qualcomm	O-QUA-SDX2-071122/7097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7098
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX2-071122/7099
Integer Overflow	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a	https://www.qualcomm	O-QUA-SDX2-071122/7100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	.com/company/product-security/bulletins/october-2022-bulletin	
Product: sdx50m_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7101
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7103
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25660		
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7105
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7106
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SDX5-071122/7107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7108
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7109
Exposure of Sensitive Information to an	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SDX5-071122/7110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	etins/october-2022-bulletin	
Product: sdx55m_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7111
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7113
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7114
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SDX5-071122/7115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	security/bulletins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7116
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7118
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7119
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7121
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7122
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SDX5-071122/7123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	r-2022-bulletin	
Product: sdx55_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7124
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7126
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7128
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7129
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7131
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7132
Time-of-check Time-of-	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of	https://www.qualcomm.com/compa	O-QUA-SDX5-071122/7133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	ny/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7134
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7136
Product: sdx57m_firmware					
Affected Version(s): -					
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7137
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX5-071122/7139
Product: sdx65_firmware					
Affected Version(s): -					
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX6-071122/7140
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX6-071122/7141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX6-071122/7142
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX6-071122/7143
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX6-071122/7144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX6-071122/7145
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDX6-071122/7146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25665		
Product: sdxr1_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7147
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7148
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer	https://www.qualcomm.com/compa	O-QUA-SDXR-071122/7149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	ny/product-security/bulletins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7150
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7152
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SDXR-071122/7153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	r-2022-bulletin	
Product: sdxr2_5g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7154
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7156
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7157
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SDXR-071122/7158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7159
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7161
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7162
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7164
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SDXR-071122/7165
Product: sd_455_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value	https://www.qualcomm.com/compa	O-QUA-SD_4-071122/7166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	ny/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_4-071122/7167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_4-071122/7168
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_4-071122/7169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Product: sd_636_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_6-071122/7170
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_6-071122/7171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_6-071122/7172
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_6-071122/7173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_6-071122/7174
Product: sd_675_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_6-071122/7175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_6-071122/7176
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_6-071122/7177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_6-071122/7178
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_6-071122/7179
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_6-071122/7180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_6-071122/7181
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_6-071122/7182
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_6-071122/7183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**		
Product: sd_8cx_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7184
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7185
Release of Invalid	19-Oct-2022	7.8	Memory corruption due to untrusted pointer	https://www.qualcomm	O-QUA-SD_8-071122/7186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7187
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7189
Product: sd_8cx_gen2_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7191
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7192
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7194
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7195
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD_8-071122/7196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	r-2022-bulletin	
Product: sd_8cx_gen3_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7197
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7199
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7200
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7202
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7203
Product: sd_8_gen1_5g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD_8-071122/7204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7205
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7207
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7208
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7209
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback	https://www.qualcomm.com/company/product-	O-QUA-SD_8-071122/7210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	security/bulletins/october-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7211
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7212
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7214
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7215
Time-of-check Time-of-	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of	https://www.qualcomm.com/compa	O-QUA-SD_8-071122/7216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	ny/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7217
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SD_8-071122/7218
Product: sg8275p_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SG82-071122/7219
Product: sg8275_firmware					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SG82-071122/7220
Product: sm4125_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM41-071122/7221
Improper Validation	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access	https://www.qualcomm.com/compa	O-QUA-SM41-071122/7222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	ny/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM41-071122/7223
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT	https://www.qualcomm.com/company/product-	O-QUA-SM41-071122/7224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM41-071122/7225
Time-of-check Time-of-	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of	https://www.qualcomm.com/compa	O-QUA-SM41-071122/7226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	ny/product-security/bulletins/october-2022-bulletin	
Product: sm4375_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM43-071122/7227
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM43-071122/7228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM43-071122/7229
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM43-071122/7230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM43-071122/7231
Product: sm6250p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM62-071122/7232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM62-071122/7233
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM62-071122/7234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM62-071122/7235
Product: sm6250_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM62-071122/7236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM62-071122/7237
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM62-071122/7238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM62-071122/7239
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM62-071122/7240
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of	https://www.qualcomm.com/company/product-security/bull	O-QUA-SM62-071122/7241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	etins/october-2022-bulletin	
Product: sm7250p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM72-071122/7242
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM72-071122/7243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM72-071122/7244
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM72-071122/7245
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM72-071122/7246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM72-071122/7247
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM72-071122/7248
Time-of-check Time-of-use	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size	https://www.qualcomm.com/company/product-	O-QUA-SM72-071122/7249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	security/bulletins/october-2022-bulletin	
Product: sm7315_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM73-071122/7250
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM73-071122/7251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM73-071122/7252
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM73-071122/7253
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM73-071122/7254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25662		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM73-071122/7255
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM73-071122/7256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM73-071122/7257
Product: sm7325p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM73-071122/7258
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SM73-071122/7259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	r-2022-bulletin	
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM73-071122/7260
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM73-071122/7261
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SM73-071122/7262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM73-071122/7263
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM73-071122/7264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM73-071122/7265
Product: sm8550_firmware					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SM85-071122/7266
Product: sw5100p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-SW51-071122/7267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	etins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7268
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7270
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7272
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7274
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7275
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7277
Product: sw5100_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25687		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7279
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7281
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7282
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens	https://www.qualcomm.com/compa	O-QUA-SW51-071122/7283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7285
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7286
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25664		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SW51-071122/7288
Product: sxr2150p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SXR2-071122/7289
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in	https://www.qualcomm.com/company/product-security/bull	O-QUA-SXR2-071122/7290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SXR2-071122/7291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-SXR2-071122/7292
Product: wcd9306_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7294
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Product: wcd9326_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7296
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7298
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7300
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7301
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCD9-071122/7302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7303
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7305
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7306
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33214		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7308
Product: wcd9330_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7309
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCD9-071122/7310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7311
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7313
Product: wcd9335_firmware					
Affected Version(s): -					
Buffer Copy without Checking	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-WCD9-071122/7314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	security/bulletins/october-2022-bulletin	
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7315
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7317
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7319
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7321
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7323
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7324
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: wcd9340_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7326
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7328
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7330
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7331
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCD9-071122/7332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	etins/octobe r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://ww w.qualcomm .com/compa ny/product-security/bull etins/octobe r-2022-bulletin	O-QUA-WCD9-071122/7333
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://ww w.qualcomm .com/compa ny/product-security/bull etins/octobe r-2022-bulletin	O-QUA-WCD9-071122/7334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7335
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7336
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7338
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7339
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: wcd9341_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7341
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7343
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7345
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7346
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7348
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7350
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7351
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7353
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7354
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22078		
Product: wcd9360_firmware					
Affected Version(s): -					
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7356
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7358
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7360
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: wcd9370_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7362
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7364
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7366
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7367
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7368
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCD9-071122/7369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7370
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-WCD9-071122/7371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	security/bulletins/october-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7372
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7373
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: wcd9371_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7375
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7377
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7379
Product: wcd9375_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25687		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7381
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7383
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7384
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCD9-071122/7385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7386
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7388
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7389
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33214		
Product: wcd9380_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7391
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7392
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer	https://www.qualcomm.com/compa	O-QUA-WCD9-071122/7393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	ny/product-security/bulletins/october-2022-bulletin	
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7394
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7395
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCD9-071122/7396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	r-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7397
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7398
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7399
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7401
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7403
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7404
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7406
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7407
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: wcd9385_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7409
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7411
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7412
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7414
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7415
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7417
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7418
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCD9-071122/7419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7420
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7421
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7423
Product: wcd9390_firmware					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCD9-071122/7424
Product: wcd9395_firmware					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCD9-071122/7425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	etins/october-2022-bulletin	
Product: wcn3610_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7426
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7428
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7430
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7431
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while	https://www.qualcomm.com/compa	O-QUA-WCN3-071122/7432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	ny/product-security/bulletins/october-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7433
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7435
Product: wcn3615_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7436
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value	https://www.qualcomm.com/compa	O-QUA-WCN3-071122/7437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	ny/product-security/bulletins/october-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7438
Integer Overflow or	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-071122/7439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7441
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7442
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN3-071122/7443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	r-2022-bulletin	
Product: wcn3620_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7444
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7446
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7448
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7449
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: wcn3660b_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7451
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7453
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7455
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7457
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7458
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN3-071122/7459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7460
Product: wcn3660_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7462
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7464
Product: wcn3680b_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7466
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7468
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7470
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7471
Time-of-check	19-Oct-2022	7	Memory corruption in display due to time-of-	https://www.qualcomm	O-QUA-WCN3-071122/7472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	.com/company/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7473
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcn3680_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7475
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7476
Improper Validation	19-Oct-2022	9.8	Memory corruption in WLAN due to out of	https://www.qualcomm	O-QUA-WCN3-071122/7477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7478
Exposure of Sensitive	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU	https://www.qualcomm.com/compa	O-QUA-WCN3-071122/7479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information to an Unauthorized Actor			reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	ny/product-security/bulletins/october-2022-bulletin	
Product: wcn3910_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7480
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7482
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7484
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33214		
Product: wcn3950_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7486
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7488
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7490
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7491
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7492
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN3-071122/7493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7494
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN3-071122/7495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	r-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7496
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7497
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: wcn3980_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7499
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7501
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7503
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7504
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-071122/7505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	etins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7506
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7508
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7509
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33214		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7511
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7512
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: wcn3988_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7514
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7516
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7518
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7520
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7521
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN3-071122/7522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7523
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7524
Product: wcn3990_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7525
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7526
Improper Validation	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access	https://www.qualcomm.com/compa	O-QUA-WCN3-071122/7527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	ny/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7528
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-WCN3-071122/7529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	security/bulletins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7530
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7531
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7533
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7535
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7536
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7538
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7539
Product: wcn3991_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7541
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7543
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7544
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7546
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7547
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**		
Product: wcn3998_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7549
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7551
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7553
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7554
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN3-071122/7555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7556
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7558
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7559
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7561
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7562
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: wcn3999_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7564
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7566
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7568
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN3-071122/7570
Product: wcn6740_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25687		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7572
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7574
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7575
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7576
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN6-071122/7577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	etins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7578
Time-of-check Time-of-use	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size	https://www.qualcomm.com/company/product-	O-QUA-WCN6-071122/7579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	security/bulletins/october-2022-bulletin	
Product: wcn6750_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7580
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7582
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7583
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25662		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7585
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7587
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7588
Product: wcn6850_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7590
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7592
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7593
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7595
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25749		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7597
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7598
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7600
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7601
Product: wcn6851_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7603
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7605
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7606
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25662		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7608
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7610
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7611
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7613
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7614
Product: wcn6855_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN6-071122/7615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	r-2022-bulletin	
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7616
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7618
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7619
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7620
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN6-071122/7621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	r-2022-bulletin	
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7622
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7623
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7624
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN6-071122/7625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7626
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN6-071122/7627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	etins/october-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7628
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7629
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7631
Product: wcn6856_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7632
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming	https://www.qualcomm.com/company/product-	O-QUA-WCN6-071122/7633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7634
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN6-071122/7635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	etins/october-2022-bulletin	
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7636
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7637
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7638
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7640
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7641
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7643
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7644
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN6-071122/7645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7646
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7647
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN6-071122/7648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Product: wcn7850_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7649
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7651
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7652
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7654
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7655
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7656
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7657
Release of Invalid	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in	https://www.qualcomm.com/compa	O-QUA-WCN7-071122/7658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	ny/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7659
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7661
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7662
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7664
Product: wcn7851_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7666
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7668
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7669
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7670
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7671
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN7-071122/7672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	etins/october-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7673
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7674
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7676
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7677
Time-of-check Time-of-	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of	https://www.qualcomm.com/compa	O-QUA-WCN7-071122/7678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	ny/product-security/bulletins/october-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7679
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WCN7-071122/7680
Product: wsa8810_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7681
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7682
Improper Validation	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access	https://www.qualcomm.com/compa	O-QUA-WSA8-071122/7683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	ny/product-security/bulletins/october-2022-bulletin	
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7684
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing	https://www.qualcomm.com/company/product-	O-QUA-WSA8-071122/7685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	security/bulletins/october-2022-bulletin	
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7686
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7687
Release of Invalid	19-Oct-2022	7.5	Information disclosure due to untrusted pointer	https://www.qualcomm	O-QUA-WSA8-071122/7688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer or Reference			dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	.com/company/product-security/bulletins/october-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7689
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7691
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7692
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WSA8-071122/7693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	r-2022-bulletin	
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7694
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7695
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WSA8-071122/7696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	r-2022-bulletin	
Product: wsa8815_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7697
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7699
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**		
Out-of-bounds Read	19-Oct-2022	9.1	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25719**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7701
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7703
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7704
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7706
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7707
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WSA8-071122/7708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	r-2022-bulletin	
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7709
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7710
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7712
Product: wsa8830_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25687		
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25718**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7714
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25720		
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25748**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7716
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7717
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25660		
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7719
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7720
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7721
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**		
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25736**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7723
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**		
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7725
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7726
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25666		
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7728
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7729
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**		
Product: wsa8835_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-2022	9.8	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25687**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7731
N/A	19-Oct-2022	9.8	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25718		
Improper Validation of Array Index	19-Oct-2022	9.8	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25720**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7733
Integer Overflow or Wraparound	19-Oct-2022	9.8	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25748		
Use After Free	19-Oct-2022	7.8	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile **CVE ID : CVE-2022-22077**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7735
Double Free	19-Oct-2022	7.8	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25660**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7736
Release of Invalid Pointer or Reference	19-Oct-2022	7.8	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-25661**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7737
Use After Free	19-Oct-2022	7.8	Memory corruption in multimedia due to use after free during callback registration failure in Snapdragon Mobile **CVE ID : CVE-2022-25723**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7738
Buffer Copy without	19-Oct-2022	7.8	Memory corruption in Qualcomm IPC due to buffer copy without	https://www.qualcomm.com/compa	O-QUA-WSA8-071122/7739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile **CVE ID : CVE-2022-33217**	ny/product-security/bulletins/october-2022-bulletin	
Release of Invalid Pointer or Reference	19-Oct-2022	7.5	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25662**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7740
Out-of-bounds Read	19-Oct-2022	7.5	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25736		
Out-of-bounds Read	19-Oct-2022	7.5	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25749**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7742
Out-of-bounds Read	19-Oct-2022	7.1	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile **CVE ID : CVE-2022-25665**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7743
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Oct-2022	7	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-33214**		
Use After Free	19-Oct-2022	6.7	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25666**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7745
Out-of-bounds Read	19-Oct-2022	5.5	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2022-25663**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7746
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2022	5.5	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25664**		
Integer Overflow or Wraparound	19-Oct-2022	4.6	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22078**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7748
Product: wsa8840_firmware					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7749
Product: wsa8845h_firmware					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WSA8-071122/7750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25750	r-2022-bulletin	
Product: wsa8845_firmware					
Affected Version(s): -					
Double Free	19-Oct-2022	8.8	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile **CVE ID : CVE-2022-25750**	https://www.qualcomm.com/company/product-security/bulletins/october-2022-bulletin	O-QUA-WSA8-071122/7751
Vendor: robustel					
Product: r1510_firmware					
Affected Version(s): 3.1.16					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	9.8	An OS command injection vulnerability exists in the sysupgrade command injection functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-32765**	N/A	O-ROB-R151-071122/7752
Improper Neutralization of Special Elements used in an OS Command ('OS	25-Oct-2022	9.8	An OS command injection vulnerability exists in the js_package install functionality of Robustel R1510 3.1.16. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of	N/A	O-ROB-R151-071122/7753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			requests to trigger this vulnerability. **CVE ID : CVE-2022-33150**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Oct-2022	9.1	A directory traversal vulnerability exists in the web_server /ajax/remove/ functionality of Robustel R1510 3.1.16. A specially-crafted network request can lead to arbitrary file deletion. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-33897**	N/A	O-ROB-R151-071122/7754
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_authorized_keys/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35261**	N/A	O-ROB-R151-071122/7755
Improper Neutralization of Special Elements used in a	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted	N/A	O-ROB-R151-071122/7756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_xml_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35262**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35263**	N/A	O-ROB-R151-071122/7757
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_aaa_cert	N/A	O-ROB-R151-071122/7758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35264**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_nodejs_app/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35265**	N/A	O-ROB-R151-071122/7759
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_firmware/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35266**	N/A	O-ROB-R151-071122/7760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_https_cert_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35267**	N/A	O-ROB-R151-071122/7761
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_sdk_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35268**	N/A	O-ROB-R151-071122/7762
Improper Neutralization of Special Elements used in a Command	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead	N/A	O-ROB-R151-071122/7763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_e2c_json_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35269**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_wireguard_cert_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35270**	N/A	O-ROB-R151-071122/7764
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_cert_file/` API is affected by	N/A	O-ROB-R151-071122/7765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection vulnerability. **CVE ID : CVE-2022-35271**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	7.2	An OS command injection vulnerability exists in the web_server /action/import_authorized_keys/ functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-34850**	N/A	O-ROB-R151-071122/7766
Insufficient Verification of Data Authenticity	25-Oct-2022	2.7	A firmware update vulnerability exists in the sysupgrade functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network packet can lead to arbitrary firmware update. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-34845**	N/A	O-ROB-R151-071122/7767
Affected Version(s): 3.3.0					
Improper Neutralization of Special Elements used in a Command ('Comma	25-Oct-2022	9.8	An OS command injection vulnerability exists in the sysupgrade command injection functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to arbitrary command	N/A	O-ROB-R151-071122/7768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
nd Injection')			execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-32765**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	9.8	An OS command injection vulnerability exists in the js_package install functionality of Robustel R1510 3.1.16. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-33150**	N/A	O-ROB-R151-071122/7769
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_authorized_keys/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35261**	N/A	O-ROB-R151-071122/7770
Improper Neutralization of Special	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel	N/A	O-ROB-R151-071122/7771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_xml_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35262**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35263**	N/A	O-ROB-R151-071122/7772
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this	N/A	O-ROB-R151-071122/7773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability.The `/action/import_aaa_cert_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35264**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_nodejs_app/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35265**	N/A	O-ROB-R151-071122/7774
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_firmware/` API is affected by command injection vulnerability.	N/A	O-ROB-R151-071122/7775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35266		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_https_cert_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35267**	N/A	O-ROB-R151-071122/7776
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_sdk_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35268**	N/A	O-ROB-R151-071122/7777
Improper Neutralization of Special	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel	N/A	O-ROB-R151-071122/7778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_e2c_json_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35269**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.The `/action/import_wireguard_cert_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35270**	N/A	O-ROB-R151-071122/7779
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2022	7.5	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this	N/A	O-ROB-R151-071122/7780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability.The `/action/import_cert_file/` API is affected by command injection vulnerability. **CVE ID : CVE-2022-35271**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Oct-2022	7.2	An OS command injection vulnerability exists in the web_server /action/import_authorized_keys/ functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-34850**	N/A	O-ROB-R151-071122/7781
Insufficient Verification of Data Authenticity	25-Oct-2022	2.7	A firmware update vulnerability exists in the sysupgrade functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network packet can lead to arbitrary firmware update. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-34845**	N/A	O-ROB-R151-071122/7782
Vendor: Tenda					
Product: 11n_firmware					
Affected Version(s): 5.07.33_cn					
Improper Authentication	20-Oct-2022	9.8	Tenda 11N with firmware version V5.07.33_cn suffers from	N/A	O-TEN-11N_-071122/7783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an Authentication Bypass vulnerability. **CVE ID : CVE-2022-42233**		
Product: ac10_firmware					
Affected Version(s): 15.03.06.23					
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/fromNatStaticSetting. **CVE ID : CVE-2022-42163**	N/A	O-TEN-AC10-071122/7784
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/formSetClientState. **CVE ID : CVE-2022-42164**	N/A	O-TEN-AC10-071122/7785
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/formSetDeviceName. **CVE ID : CVE-2022-42165**	N/A	O-TEN-AC10-071122/7786
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/formSetSpeedWan. **CVE ID : CVE-2022-42166**	N/A	O-TEN-AC10-071122/7787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/formSetFirewallCfg. **CVE ID : CVE-2022-42167**	N/A	O-TEN-AC10-071122/7788
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/fromSetIpMacBind. **CVE ID : CVE-2022-42168**	N/A	O-TEN-AC10-071122/7789
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/addWifiMacFilter. **CVE ID : CVE-2022-42169**	N/A	O-TEN-AC10-071122/7790
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/formWifiWpsStart. **CVE ID : CVE-2022-42170**	N/A	O-TEN-AC10-071122/7791
Out-of-bounds Write	17-Oct-2022	9.8	Tenda AC10 V15.03.06.23 contains a Stack overflow vulnerability via /goform/saveParentControlInfo. **CVE ID : CVE-2022-42171**	N/A	O-TEN-AC10-071122/7792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ac15_firmware					
Affected Version(s): 15.03.05.18					
Out-of-bounds Write	18-Oct-2022	7.5	Tenda AC15 V15.03.05.18 was discovered to contain a stack overflow via the timeZone parameter in the form_fast_setting_wifi_set function. **CVE ID : CVE-2022-43259**	N/A	O-TEN-AC15-071122/7793
Affected Version(s): 15.03.05.19					
Out-of-bounds Write	18-Oct-2022	7.5	Tenda AC15 V15.03.05.18 was discovered to contain a stack overflow via the timeZone parameter in the form_fast_setting_wifi_set function. **CVE ID : CVE-2022-43259**	N/A	O-TEN-AC15-071122/7794
Product: ac18_firmware					
Affected Version(s): 15.03.05.19					
Out-of-bounds Write	18-Oct-2022	9.8	Tenda AC18 V15.03.05.19(6318) was discovered to contain a stack overflow via the time parameter in the fromSetSysTime function. **CVE ID : CVE-2022-43260**	N/A	O-TEN-AC18-071122/7795
Product: ax1803_firmware					
Affected Version(s): 1.0.0.1					
Out-of-bounds Write	27-Oct-2022	9.8	In Tenda ax1803 v1.0.0.1, the http requests handled by the	N/A	O-TEN-AX18-071122/7796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fromAdvSetMacMtuWan functions, wanSpeed, cloneType, mac, can cause a stack overflow and enable remote code execution (RCE). **CVE ID : CVE-2022-40876**		
Out-of-bounds Write	27-Oct-2022	7.5	Tenda AX1803 v1.0.0.1 was discovered to contain a heap overflow vulnerability in the GetParentControlInfo function, which can cause a denial of service attack through a carefully constructed http request. **CVE ID : CVE-2022-40874**	N/A	O-TEN-AX18-071122/7797
Out-of-bounds Write	27-Oct-2022	7.5	Tenda AX1803 v1.0.0.1 was discovered to contain a heap overflow in the function GetParentControlInfo. **CVE ID : CVE-2022-40875**	N/A	O-TEN-AX18-071122/7798
Product: tx3_firmware					
Affected Version(s): 16.03.13.11					
Out-of-bounds Write	19-Oct-2022	9.8	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the list parameter at /goform/SetVirtualServerCfg. **CVE ID : CVE-2022-43024**	N/A	O-TEN-TX3_-071122/7799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2022	9.8	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the startIp parameter at /goform/SetPptpServerCfg. **CVE ID : CVE-2022-43025**	N/A	O-TEN-TX3_-071122/7800
Out-of-bounds Write	19-Oct-2022	9.8	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the endIp parameter at /goform/SetPptpServerCfg. **CVE ID : CVE-2022-43026**	N/A	O-TEN-TX3_-071122/7801
Out-of-bounds Write	19-Oct-2022	9.8	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the firewallEn parameter at /goform/SetFirewallCfg. **CVE ID : CVE-2022-43027**	N/A	O-TEN-TX3_-071122/7802
Out-of-bounds Write	19-Oct-2022	9.8	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the timeZone parameter at /goform/SetSysTimeCfg. **CVE ID : CVE-2022-43028**	N/A	O-TEN-TX3_-071122/7803
Out-of-bounds Write	19-Oct-2022	9.8	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was	N/A	O-TEN-TX3_-071122/7804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a stack overflow via the time parameter at /goform/SetSysTimeCfg. **CVE ID : CVE-2022-43029**		
Vendor: Tp-link					
Product: ax10_firmware					
Affected Version(s): v1_211117					
Authentication Bypass by Capture-replay	18-Oct-2022	8.1	TP-Link AX10v1 V1_211117 allows attackers to execute a replay attack by using a previously transmitted encrypted authentication message and valid authentication token. Attackers are able to login to the web application as an admin user. **CVE ID : CVE-2022-41541**	https://www.tp-link.com/us/support/download/archer-ax10/v1/#Firmware	O-TP--AX10-071122/7805
Use of Hard-coded Credentials	18-Oct-2022	5.9	The web app client of TP-Link AX10v1 V1_211117 uses hard-coded cryptographic keys when communicating with the router. Attackers who are able to intercept the communications between the web client and router through a man-in-the-middle attack can then obtain the sequence key via a brute-force attack, and access sensitive information. **CVE ID : CVE-2022-41540**	https://www.tp-link.com/us/support/download/archer-ax10/v1/#Firmware	O-TP--AX10-071122/7806
Product: tl-wr841n_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 4.17.16_build_120201_rel.54750n					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2022	6.1	TP-Link TL-WR841N 8.0 4.17.16 Build 120201 Rel.54750n is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2022-42202**	N/A	O-TP--TL-W-071122/7807
Vendor: Wago					
Product: 750-8100_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7808
Product: 750-8101\/000-010_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8101\/025-000_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7810
Product: 750-8101_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8102\/025-000_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7812
Product: 750-8102_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8202\/000-011_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7814
Product: 750-8202\/000-012_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter.	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3281		
Product: 750-8202\/000-022_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7816
Product: 750-8202\/040-000_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7817
Product: 750-8206\/025-000_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7818
Product: 750-8206\/025-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7819
Product: 750-8206\/040-000_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series	https://cert.vde.com/en/	O-WAG-750--071122/7820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	advisories/VDE-2022-042/	
Product: 750-8206\/040-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7821
Product: 750-8206_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8207\/025-000_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7823
Product: 750-8207\/025-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8207_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7825
Product: 750-8208\/025-000_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8208\/025-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7827
Product: 750-8208_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8210\/025-000_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7829
Product: 750-8210\/040-000_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter.	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3281		
Product: 750-8210_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7831
Product: 750-8211\/040-000_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7832
Product: 750-8211_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7833
Product: 750-8212\/000-100_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7834
Product: 750-8212\/025-000_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series	https://cert.vde.com/en/	O-WAG-750--071122/7835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	advisories/VDE-2022-042/	
Product: 750-8212\/025-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7836
Product: 750-8212\/025-002_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8212\/040-000_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7838
Product: 750-8212\/040-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8212\/040-010_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7840
Product: 750-8212_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8213\/040-010_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7842
Product: 750-8213_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8214_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7844
Product: 750-8215_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter.	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3281		
Product: 750-8216\/025-000_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7846
Product: 750-8216\/025-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7847
Product: 750-8216\/040-000_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7848
Product: 750-8216_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7849
Product: 750-8217\/025-000_firmware					
Affected Version(s): From (including) 03.04.10\\(16\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series	https://cert.vde.com/en/	O-WAG-750--071122/7850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	advisories/VDE-2022-042/	
Product: 750-8217\/600-000_firmware					
Affected Version(s): From (including) 03.04.10\\(16\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7851
Product: 750-8217\/625-000_firmware					
Affected Version(s): From (including) 03.04.10\\(16\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 750-8217_firmware					
Affected Version(s): From (including) 03.04.10\\(16\\) Up to (including) 03.10.08\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-750--071122/7853
Product: 751-9301_firmware					
Affected Version(s): From (including) 03.07.17\\(19\\) Up to (including) 03.09.08\\(21\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-751--071122/7854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 752-8303\/8000-002_firmware					
Affected Version(s): From (including) 03.06.09\\(18\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-752--071122/7855
Product: 762-4101_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-4102_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7857
Product: 762-4103_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-4104_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7859
Product: 762-4201\/8000-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter.	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3281		
Product: 762-4202\/8000-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7861
Product: 762-4203\/8000-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7862
Product: 762-4204\/8000-001_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7863
Product: 762-4205\/8000-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7864
Product: 762-4206\/8000-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series	https://cert.vde.com/en/	O-WAG-762--071122/7865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	advisories/VDE-2022-042/	
Product: 762-4301\/8000-002_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7866
Product: 762-4302\/8000-002_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-4303\/8000-002_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7868
Product: 762-4304\/8000-002_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-5203\/8000-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7870
Product: 762-5204\/8000-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-5205\/8000-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7872
Product: 762-5206\/8000-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-5303\/8000-002_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7874
Product: 762-5304\/8000-002_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter.	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3281		
Product: 762-5305\/8000-002_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7876
Product: 762-5306\/8000-002_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7877
Product: 762-6201\/8000-001_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7878
Product: 762-6202\/8000-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7879
Product: 762-6203\/8000-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series	https://cert.vde.com/en/	O-WAG-762--071122/7880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	advisories/VDE-2022-042/	
Product: 762-6204\/8000-001_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7881
Product: 762-6301\/8000-002_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-6302\/8000-002_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7883
Product: 762-6303\/8000-002_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**		
Product: 762-6304\/8000-002_firmware					
Affected Version(s): From (including) 03.01.07\\(13\\) Up to (including) 03.10.09\\(22\\)					
N/A	17-Oct-2022	7.5	WAGO Series PFC100/PFC200, Series Touch Panel 600, Compact Controller CC100 and Edge Controller in multiple versions are prone to a loss of MAC-Address-Filtering after reboot. This may allow an remote attacker to circumvent the reach the network that should be protected by the MAC address filter. **CVE ID : CVE-2022-3281**	https://cert.vde.com/en/advisories/VDE-2022-042/	O-WAG-762--071122/7885