National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures(CVE) Report
01 - 15 Feb 2023 Vol. 10 No. 03

Table of Content

Vendor	Product	Page Number
Application		
a3rev	page_view_count	1
actionpack_project	actionpack	1
activerecord_project	activerecord	2
activesupport_project	activesupport	3
agentejo	cockpit	4
akindo-sushiro	hong_kong_sushiro	5
	singapore_sushiro	6
	sushiro	6
	taiwan_sushiro	7
	thailand_sushiro	7
Amazon	opensearch	8
amazonjs_project	amazonjs	9
Ampache	ampache	10
anchore	syft	11
answer	answer	13
Apache	inlong	15
	kafka	16
	nifi	19
	sling_cms	19
	sling_jcr_base	20
art_gallery_management_system_project	art_gallery_management_system	20
Atlassian	jira_service_management	21
best_online_news_portal_project	best_online_news_portal	25
bgerp	bgerp	26
bplugins	html5_audio_player	26

Vendor	Product	Page Number
Brave	adblock-lists	27
btcpayserver	btcpayserver	27
butterfly-button_project	butterfly-button	28
calendar_event_management_system_project	calendar_event_management_system	29
canteen_management_system_project	canteen_management_system	30
caphyon	advanced_installer	31
chikoi_project	chikoi	31
churchcrm	churchcrm	32
Cisco	iox	33
cloak_front_end_email_project	cloak_front_end_email	33
clockwork_web_project	clockwork_web	34
cncf	opentelemetry-go_contrib	35
connectwise	automate	36
	connectwise	37
	control	38
couchbase	couchbase_server	39
cozmoslabs	profile_builder	40
crocoblock	jetwidgets_for_elementor	40
cryptography_project	cryptography	41
cusrev	customer_reviews_for_woocommerce	41
datahub_project	datahub	42
Dell	alienware_command_center	48
	alienware_update	48
	command_update	49
	command_|_integration_suite_for_system_center	50
	command_|_intel_vpro_out_of_band	50
	command_|_monitor	51
	emc_networker	51
deltaww	diascreen	52

Vendor	Product	Page Number
deltaww	dopsoft	53
devolutions	devolutions_server	54
devowl	wordpress_real_media_library	54
discourse	discourse	55
Djangoproject	django	66
dompdf_project	dompdf	69
dst-admin_project	dst-admin	71
easynas	easynas	73
Eclipse	vert.x-web	74
editorconfig	editorconfig	75
elecom	camera_assistant	75
	quickfiledealer	76
employee_leaves_management_system_project	employee_leaves_management_system	76
eta.js	eta	77
exactmetrics	exactmetrics	77
Expressionengine	expressionengine	78
F5	big-ip_access_policy_manager	78
	big-ip_advanced_firewall_manager	105
	big-ip_advanced_web_application_firewall	128
	big-ip_analytics	131
	big-ip_application_acceleration_manager	151
	big-ip_application_security_manager	169
	big-ip_ddos_hybrid_defender	192
	big-ip_domain_name_system	209
	big-ip_edge	229
	big-ip_fraud_protection_service	230
	big-ip_link_controller	248
	big-ip_local_traffic_manager	268
	big-ip_policy_enforcement_manager	291
	big-ip_service_proxy	312
	big-ip_ssl_orchestrator	313
farsight	provide_server	333

Vendor	Product	Page Number
fastcms_project	fastcms	334
fastify	fastify-multipart	334
flexible_captcha_project	flexible_captcha	336
Foliovision	fv_flowplayer_video_player	336
forget_heart_message_box_project	forget_heart_message_box	336
formwork_project	formwork	337
fortra	goanywhere_managed_file_transfer	337
Froxlor	froxlor	338
ftdms_project	ftdms	338
Fujitsu	tsclinical_define.xml_generator	339
	tsclinical_metadata_desktop_tools	339
gamipress	gamipress	340
getlasso	simple_urls	340
getwpfunnels	drag_\&_drop_sales_funnel_builder	341
Git-scm	git	341
git_for_windows_project	git_for_windows	363
GNU	glibc	365
	gnutls	366
Google	chrome	367
gpac	gpac	370
gptaipower	gpt_ai_power	372
gss-ntlmssp_project	gss-ntlmssp	373
hapi	formula	377
happyforms	happyforms	377
Haproxy	haproxy	378
harfbuzz_project	harfbuzz	382
hashicorp	boundary	383
helm	helm	383
IBM	cloud_pak_for_business_automation	384
	infosphere_information_server	386
	websphere_application_server	387
ichiranusa	ichiran	387

Vendor	Product	Page Number
in2code	femanager	388
interactive_geo_maps_project	interactive_geo_maps	390
inventory_management_system_project	inventory_management_system	391
invoiceplane	invoiceplane	393
Ipython	ipython	393
jellyfin	jellyfin	394
Jenkins	azure_credentials	395
	email_extension	396
	junit	397
	pipeline\	397
	synopsys_coverity	398
jfinaloa_project	jfinaloa	400
jflyfox	jfinal_cms	400
Joomla	joomla\!	400
json-parser_project	json-parser	401
judge	product_reviews_for_woocommerce	401
kardex	kardex_control_center	402
kiwitcms	kiwi_tcms	403
Kodi	kodi	404
kraken	kraken.io_image_optimizer	405
libpeconv_project	libpeconv	405
Libtiff	libtiff	405
lightspeedhq	ecwid_ecommerce_shopping_cart	410
Linuxfoundation	argo_continuous_delivery	410
	backstage_catalog-model	412
	backstage_core-components	413
	backstage_plugin-catalog-backend	414
ljapps	wp_airbnb_review_slider	416
	wp_google_review_slider	416
	wp_review_slider	417
	wp_tripadvisor_review_slider	417

Vendor	Product	Page Number
ljapps	wp_yelp_review_slider	417
lmxcms	lmxcms	418
mage-people	event_manager_and_tickets_selling_for_woocommerce	418
marmelab	ra-ui-materialui	419
	react-admin	421
material_design_icons_for_page_builders_project	material_design_icons_for_page_builders	423
mediacp	media_control_panel	423
medical_certificate_generator_app_project	medical_certificate_generator_app	424
mendix	mendix	425
Microsoft	.net	430
	365_apps	434
	3d_builder	434
	azure_app_service_on_azure_stack	434
	azure_data_box_gateway	435
	azure_machine_learning	435
	azure_stack_edge	435
	defender_for_iot	435
	defender_security_intelligence_updates	435
	dynamics_365	436
	edge_chromium	438
	exchange_server	439
	office	441
	office_long_term_servicing_channel	441
	office_online_server	441
	office_web_apps	442
	onenote	442
	power_bi_report_server	442
	print_3d	442
	sharepoint_enterprise_server	443
	sharepoint_foundation	443

Vendor	Product	Page Number
Microsoft	sharepoint_server	444
	sql_server	444
	sql_server_2019_integration_services	450
	sql_server_2022_integration_services	450
	visual_studio_2017	451
	visual_studio_2019	452
	visual_studio_2022	452
	word	455
Microweber	microweber	455
Mitel	micontact_center_business	456
modoboa	modoboa	456
mojojson_project	mojojson	457
mojoportal	mojoportal	457
monsterinsights	monsterinsights	459
naver_map_project	naver_map	459
NEC	pc_settings_tool	460
Nextcloud	desktop	460
	mail	461
	nextcloud_server	465
	richdocuments	471
nosh_chartingsystem_project	nosh_chartingsystem	477
objectcomputing	opendds	477
okfn	ckan	478
onedev_project	onedev	480
online_eyewear_shop_project	online_eyewear_shop	480
online_food_ordering_system_project	online_food_ordering_system	482
open5gs	open5gs	484
Openssh	openssh	485
Openssl	openssl	486
Opensuse	libzypp-plugin-appdata	497

Vendor	Product	Page Number
openzeppelin	contracts	498
orangescrum	orangescrum	499
Owncloud	owncloud	500
palletsprojects	werkzeug	501
Paloaltonetworks	cortex_xdr_agent	503
	cortex_xsoar	504
parseplatform	parse-server	505
pdfio_project	pdfio	506
phpcrazy_project	phpcrazy	507
Phpipam	phpipam	508
Phpmyadmin	phpmyadmin	509
Phpmyfaq	phpmyfaq	510
pickplugins	product_slider_for_woocommerce	513
Pimcore	pimcore	513
pinpoint	pinpoint_booking_system	515
plugin	yourchannel	515
priority-software	priority	515
Progress	ws_ftp_server	516
Projectsend	projectsend	516
protocol	go-bitfield	517
	go-unixfs	518
	go-unixfsnode	518
pterodactyl	wings	519
rafflepress	giveaways_and_contests_by_rafflepress	527
raffle_draw_system_project	raffle_draw_system	528
Rapid7	metasploit	529
reason-jose_project	reason-jose	530
rebelcode	spotlight_social_feeds	530
redpanda	redpanda	531
responsivevoice	responsivevoice_text_to_speech	532
responsive_gallery_grid_project	responsive_gallery_grid	533

Vendor	Product	Page Number
rextheme	wp_vr	533
Ruby-lang	Ruby	534
Rubyonrails	globalid	534
	rails	535
Ruckuswireless	ruckus_wireless_admin	539
Samsung	bixby_vision	540
	cloud	540
	flow	540
	galaxy_store	541
	one_hand_operation_\+	541
	smart_things	542
SAP	businessobjects_business_intelligence_platform	542
	business_objects_business_intelligence_platform	544
	business_planning_and_consolidation	545
	customer_relationship_management_webclient_ui	546
	fiori	550
	grc_process_control	550
	host_agent	554
	netweaver_application_server_abap	555
	netweaver_as_abap_business_server_pages	588
	s4fnd	603
	solution_manager	604
	s\/4hana	605
selfwealth	selfwealth	606
send_pdf_for_contact_form_7_project	send_pdf_for_contact_form_7	607
shapedplugin	location_weather	607
	wp_tabs	608
Shopex	ecshop	608
Shopware	swagpaypal	608

Vendor	Product	Page Number
shortpixel	enable_media_replace	609
Siemens	comos	609
	parasolid	615
	solid_edge	617
	solid_edge_se2023	618
	tecnomatix_plant_simulation	627
simple_sales_management_system_project	simple_sales_management_system	635
siteground	siteground_security	636
slims_project	slims	636
smartwp	lightweight_accordion	636
Solarwinds	orion_platform	637
Sonicwall	email_security	637
Southrivertech	titan_ftp_server	638
Splunk	add-on_builder	638
	cloudconnect_software_development_kit	639
	splunk	640
	splunk_cloud_platform	655
squidex.io	squidex	660
starliteproject	starlite	661
switcherapi	switcher_client	662
synopsys	coverity	663
templatesnext	templatesnext_toolkit	664
Tenable	nessus	664
	tenable.io	665
	tenable.sc	666
themeum	tutor_lms	667
themify	portfolio_post	667
timescale	timescaledb	667
tina	tinacms	669
Tipsandtricks-hq	easy_accept_payments_for_paypal	670
trellix	data_loss_prevention	670
Trendmicro	apex_one	671

Vendor	Product	Page Number
twinpictures	annual_archive	671
	jquery_t\(-\)_countdown_widget	672
Typo3	typo3	672
ureport_project	ureport	683
utubevideo_gallery_project	utubevideo_gallery	684
Vbulletin	vbulletin	684
vilyon	gallery_factory_lite	686
vimeo_video_autoplay_automute_project	vimeo_video_autoplay_automute	686
Vmware	vrealize_operations	687
	workstation	687
wallabag	wallabag	688
wallix	bastion_access_manager	689
wcvendors	wc_vendors_marketplace	690
webberzone	contextual_related_posts	690
wickedplugins	wicked_folders	690
wordprezi_project	wordprezi	702
wpdevart	social_like_box_and_page	703
wpfactory	ean_for_woocommerce	703
wprealize	extensive_vc_addons_for_wpbakery_page_builder	704
xuxueli	xxl-job	704
yamaps_project	yamaps	705
yetanotherforum	yaf.net	705
yugabyte	yugabytedb	706
	yugabytedb_managed	706
zippy	zstore	708
Zohocorp	manageengine_assetexplorer	708
	manageengine_servicedesk_plus	708
	manageengine_supportcenter_plus	709
	zoho_forms	709
Zulip	zulip_server	710

Vendor	Product	Page Number
Hardware		
arraynetworks	ag1000	711
	ag1000t	712
	ag1000v5	712
	ag1100v5	713
	ag1150	713
	ag1200	714
	ag1200v5	714
	ag1500	715
	ag1500fips	716
	ag1500v5	716
	ag1600	717
	ag1600v5	717
	vxag	718
baicells	neutrino_430	718
	nova430e	719
	nova430l	720
	nova436q	720
bdcom	1704-wgl	721
bosswerk	inverter	721
Cisco	807_industrial_integrated_services_router	722
	809_industrial_integrated_services_router	723
	829_industrial_integrated_services_router	724
	cgr1000	725
	cgr1240	726
	ic3000_industrial_compute_gateway	726
	ir510_wpan	727
contec	solarview_compact	728
controlbyweb	x-400	728
	x-600m	729
D-link	dir-605l	729
	dwl-2600ap	731

Vendor	Product	Page Number
deyeinverter	inverter	732
F5	big-ip_10000s	733
	big-ip_10200v	733
	big-ip_10200v-ssl	734
	big-ip_12000	735
	big-ip_5000s	735
	big-ip_5200v	736
	big-ip_5200v-ssl	736
	big-ip_7000s	737
	big-ip_7200v	738
	big-ip_7200v-ssl	738
	big-ip_i10600	739
	big-ip_i10800	740
	big-ip_i11600	740
	big-ip_i11800	741
	big-ip_i15600	741
	big-ip_i15800	742
	big-ip_i5600	743
	big-ip_i5800	743
	big-ip_i7600	744
	big-ip_i7800	745
	r10600	745
	r10800	746
	r10900	746
	r5600	747
	r5800	748
	r5900	748
	velos_bx110	749
	viprion_b2100	750
	viprion_b2150	750
	viprion_b2250	751
	viprion_b4300	751

Vendor	Product	Page Number
F5	viprion_b4450	752
ls-electric	xbc-dn32u	753
mediatek	mt6580	755
	mt6731	756
	mt6735	757
	mt6737	759
	mt6739	761
	mt6753	764
	mt6757	766
	mt6757c	767
	mt6757cd	769
	mt6757ch	770
	mt6761	771
	mt6762	775
	mt6763	779
	mt6765	781
	mt6768	785
	mt6769	790
	mt6771	793
	mt6779	796
	mt6781	801
	mt6785	806
	mt6789	810
	mt6833	814
	mt6853	819
	mt6853t	824
	mt6855	826
	mt6873	830
	mt6875	835
	mt6877	838
	mt6879	843
	mt6883	847

Vendor	Product	Page Number
mediatek	mt6885	851
	mt6889	856
	mt6891	861
	mt6893	864
	mt6895	869
	mt6983	873
	mt8167	877
	mt8168	878
	mt8183	879
	mt8185	880
	mt8321	881
	mt8362a	883
	mt8365	883
	mt8385	885
	mt8666	887
	mt8667	888
	mt8675	888
	mt8765	889
	mt8766	892
	mt8768	894
	mt8786	897
	mt8788	900
	mt8789	902
	mt8791	905
	mt8791t	908
	mt8797	910
multilaser	re057	914
	re170	914
Netgear	d6100	915
	dgn1000v3	916
	prosafe_fs726tp	917
	r8900	917

Vendor	Product	Page Number
Netgear	r9000	918
	wndr3700	919
	wnr1000v2	921
	wnr2200	922
	wnr2500	923
	wnr612v2	924
	xavn2001v2	925
onekey	onekey_mini	926
	onekey_touch	926
Planex	cs-wmv02g	927
revolt-power	inverter	928
Ruckuswireless	e510	929
	h320	929
	h350	930
	h500	930
	h510	931
	h550	931
	m510	931
	m510-jp	932
	p300	932
	q410	932
	q710	933
	q910	933
	r300	933
	r310	934
	r320	934
	r350	934
	r500	935
	r510	935
	r550	935
	r560	936
	r600	936

Vendor	Product	Page Number
Ruckuswireless	r610	936
	r650	937
	r700	937
	r710	938
	r720	938
	r730	938
	r750	939
	r760	939
	r850	939
	sz-144	940
	sz-144-federal	940
	sz100	940
	sz300	941
	sz300-federal	941
	t300	941
	t301n	942
	t301s	942
	t310c	942
	t310d	943
	t310n	943
	t310s	943
	t350c	944
	t350d	944
	t350se	945
	t504	945
	t610	945
	t710	946
	t710s	946
	t750	946
	t750se	947
	t811-cm	947
	t811-cm\(non-spf\)	947

Vendor	Product	Page Number
Ruckuswireless	zd1000	948
	zd1100	948
	zd1200	948
	zd3000	949
	zd5000	949
sunellsecurity	sn-adr3804e1	949
	sn-adr3808e1	950
	sn-adr3808e2	950
	sn-adr3816e1	951
	sn-adr3816e2	951
	sn-xvr3804e1	952
	sn-xvr3808e2	952
Tenda	ac23	953
totolink	a7100ru	953
	ca300-poe	954
	t8	958
Trendnet	tew-652brp	960
	tew-811dru	962
	tv-ip651wi	965
ui	af-2x	965
	er-10x	966
	er-12	966
	er-12p	967
	er-4	967
	er-6p	968
	er-8-xg	968
	er-x	969
	er-x-sfp	969
	usg	970
	usg-pro-4	970
Operating System		
ami	megarac_sp-x	971

Vendor	Product	Page Number
Apple	iphone_os	972
	macos	973
arraynetworks	arrayos_ag	973
baicells	neutrino_430_firmware	974
	nova430e_firmware	974
	nova430l_firmware	975
	nova436q_firmware	976
bdcom	1704-wgl_firmware	976
bosswerk	inverter_firmware	977
Cisco	807_industrial_integrated_services_router_firmware	979
	809_industrial_integrated_services_router_firmware	987
	829_industrial_integrated_services_router_firmware	996
	cgr1000_firmware	1004
	cgr1240_firmware	1005
	ios_xe	1006
	ir510_wpan_firmware	1008
contec	solarview_compact_firmware	1009
controlbyweb	x-400_firmware	1009
	x-600m_firmware	1010
D-link	dwl-2600ap_firmware	1010
Debian	debian_linux	1010
Dell	emc_data_domain_os	1013
	emc_powerscale_onefs	1015
	enterprise_sonic_distribution	1019
deyeinverter	inverter_firmware	1020
Dlink	dir-605l_firmware	1021
F5	big-ip_10000s_firmware	1024
	big-ip_10200v-ssl_firmware	1024
	big-ip_10200v_firmware	1025
	big-ip_12000_firmware	1026

Vendor	Product	Page Number
F5	big-ip_5000s_firmware	1026
	big-ip_5200v-ssl_firmware	1027
	big-ip_5200v_firmware	1028
	big-ip_7000s_firmware	1028
	big-ip_7200v-ssl_firmware	1029
	big-ip_7200v_firmware	1029
	big-ip_i10600_firmware	1030
	big-ip_i10800_firmware	1031
	big-ip_i11600_firmware	1031
	big-ip_i11800_firmware	1032
	big-ip_i15600_firmware	1032
	big-ip_i15800_firmware	1033
	big-ip_i5600_firmware	1034
	big-ip_i5800_firmware	1034
	big-ip_i7600_firmware	1035
	big-ip_i7800_firmware	1036
	f5os-a	1036
	f5os-c	1037
	r10600_firmware	1037
	r10800_firmware	1038
	r10900_firmware	1038
	r5600_firmware	1039
	r5800_firmware	1040
	r5900_firmware	1040
	velos_bx110_firmware	1041
	viprion_b2100_firmware	1041
	viprion_b2150_firmware	1042
	viprion_b2250_firmware	1043
	viprion_b4300_firmware	1043
	viprion_b4450_firmware	1044
Fedoraproject	fedora	1045
Freebsd	freebsd	1045

Vendor	Product	Page Number
Google	android	1047
HP	hp-ux	1065
IBM	aix	1065
	i	1066
	z\/os	1066
Linux	linux_kernel	1066
ls-electric	xbc-dn32u_firmware	1069
Microsoft	azure_devops_server	1071
	windows	1072
	windows_10	1075
	windows_10_1507	1079
	windows_10_1511	1081
	windows_10_1607	1082
	windows_10_1703	1088
	windows_10_1709	1089
	windows_10_1803	1089
	windows_10_1807	1089
	windows_10_1809	1090
	windows_10_1903	1096
	windows_10_1909	1097
	windows_10_2004	1097
	windows_10_20h2	1097
	windows_10_21h1	1104
	windows_10_21h2	1104
	windows_10_22h2	1111
	windows_11_21h2	1117
	windows_11_22h2	1123
	windows_server_2008	1129
	windows_server_2012	1141
	windows_server_2016	1153
	windows_server_2019	1159
	windows_server_2022	1165

Vendor	Product	Page Number
multilaser	re057_firmware	1171
	re170_firmware	1172
Netgear	d6100_firmware	1173
	dgn1000v3_firmware	1174
	prosafe_fs726tp_firmware	1175
	r8900_firmware	1175
	r9000_firmware	1176
	wndr3700_firmware	1177
	wnr1000v2_firmware	1179
	wnr2200_firmware	1180
	wnr2500_firmware	1181
	wnr612v2_firmware	1182
	xavn2001v2_firmware	1183
onekey	onekey_mini_firmware	1184
	onekey_touch_firmware	1184
Opensuse	leap	1185
Oracle	solaris	1186
Planex	cs-wmv02g	1186
	cs-wmv02g_firmware	1187
Redhat	enterprise_linux	1188
revolt-power	inverter_firmware	1189
Ruckuswireless	smartzone	1191
	smartzone_ap	1192
Samsung	android	1193
sunellsecurity	sn-adr3804e1_firmware	1209
	sn-adr3808e1_firmware	1209
	sn-adr3808e2_firmware	1210
	sn-adr3816e1_firmware	1210
	sn-adr3816e2_firmware	1211
	sn-xvr3804e1_firmware	1211
	sn-xvr3808e2_firmware	1212
Suse	suse_linux_enterprise_server	1212

Vendor	Product	Page Number
Tenda	ac23_firmware	1213
totolink	a7100ru_firmware	1214
	ca300-poe_firmware	1214
	t8_firmware	1218
Trendnet	tew-652brp_firmware	1220
	tew-811dru_firmware	1222
	tv-ip651wi_firmware	1225
ui	af-2x_firmware	1225
	er-10x_firmware	1226
	er-12p_firmware	1227
	er-12_firmware	1228
	er-4_firmware	1229
	er-6p_firmware	1230
	er-8-xg_firmware	1231
	er-x-sfp_firmware	1232
	er-x_firmware	1233
	usg-pro-4_firmware	1234
	usg_firmware	1234

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: a3rev					
Product: page_view_count					
Affected Version(s): * Up to (excluding) 2.6.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The Page View Count WordPress plugin before 2.6.1 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0095**	N/A	A-A3R-PAGE-270223/1
Vendor: actionpack_project					
Product: actionpack					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.4.1					
URL Redirection to Untrusted Site ('Open Redirect')	09-Feb-2023	6.1	An open redirect vulnerability is fixed in Rails 7.0.4.1 with the new protection against open redirects from calling redirect_to with untrusted user input. In prior versions the developer was fully responsible for only providing trusted input. However the check introduced could allow an attacker to bypass with a carefully crafted URL resulting in an	N/A	A-ACT-ACTI-270223/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			open redirect vulnerability. **CVE ID : CVE-2023-22797**		
Vendor: activerecord_project					
Product: activerecord					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.4.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Feb-2023	8.8	A vulnerability in ActiveRecord <6.0.6.1, v6.1.7.1 and v7.0.4.1 related to the sanitization of comments. If malicious user input is passed to either the `annotate` query method, the `optimizer_hints` query method, or through the QueryLogs interface which automatically adds annotations, it may be sent to the database withinsufficient sanitization and be able to inject SQL outside of the comment. **CVE ID : CVE-2023-22794**	https://discuss.rubyonrails.org/t/cve-2023-22794-sql-injection-vulnerability-via-activerecord-comments/82117	A-ACT-ACTI-270223/3
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.6.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Feb-2023	8.8	A vulnerability in ActiveRecord <6.0.6.1, v6.1.7.1 and v7.0.4.1 related to the sanitization of comments. If malicious user input is passed to either the `annotate` query method, the `optimizer_hints` query method, or through the	https://discuss.rubyonrails.org/t/cve-2023-22794-sql-injection-vulnerability-via-activerecord-	A-ACT-ACTI-270223/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QueryLogs interface which automatically adds annotations, it may be sent to the database withinsufficient sanitization and be able to inject SQL outside of the comment. **CVE ID : CVE-2023-22794**	comments/82117	
Affected Version(s): From (including) 6.1.0 Up to (excluding) 6.1.7.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Feb-2023	8.8	A vulnerability in ActiveRecord <6.0.6.1, v6.1.7.1 and v7.0.4.1 related to the sanitization of comments. If malicious user input is passed to either the `annotate` query method, the `optimizer_hints` query method, or through the QueryLogs interface which automatically adds annotations, it may be sent to the database withinsufficient sanitization and be able to inject SQL outside of the comment. **CVE ID : CVE-2023-22794**	https://discuss.rubyonrails.org/t/cve-2023-22794-sql-injection-vulnerability-via-activerecord-comments/82117	A-ACT-ACTI-270223/5
Vendor: activesupport_project					
Product: activesupport					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.4.1					
N/A	09-Feb-2023	7.5	A regular expression based DoS vulnerability in Active Support <6.1.7.1 and <7.0.4.1. A	https://discuss.rubyonrails.org/t/cve-2023-	A-ACT-ACTI-270223/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted string passed to the underscore method can cause the regular expression engine to enter a state of catastrophic backtracking. This can cause the process to use large amounts of CPU and memory, leading to a possible DoS vulnerability. **CVE ID : CVE-2023-22796**	22796-possible-redos-based-dos-vulnerability-in-active-supports-underscore/82116	
Affected Version(s): * Up to (excluding) 6.1.7.1					
N/A	09-Feb-2023	7.5	A regular expression based DoS vulnerability in Active Support <6.1.7.1 and <7.0.4.1. A specially crafted string passed to the underscore method can cause the regular expression engine to enter a state of catastrophic backtracking. This can cause the process to use large amounts of CPU and memory, leading to a possible DoS vulnerability. **CVE ID : CVE-2023-22796**	https://discuss.rubyonrails.org/t/cve-2023-22796-possible-redos-based-dos-vulnerability-in-active-supports-underscore/82116	A-ACT-ACTI-270223/7
Vendor: agentejo					
Product: cockpit					
Affected Version(s): * Up to (excluding) 2.3.8					
Privilege Chaining	09-Feb-2023	8.8	Privilege Chaining in GitHub repository	https://github.com/cockpit-	A-AGE-COCK-270223/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cockpit-hq/cockpit prior to 2.3.8. **CVE ID : CVE-2023-0759**	hq/cockpit/commit/78d6ed3bf093ee11356ba66320c628c727068714, https://hunter.dev/bounties/49e2cccc-bb56-4633-ba6a-b3803e251347	
Affected Version(s): * Up to (excluding) 2.3.9					
Improper Restriction of Rendered UI Layers or Frames	11-Feb-2023	5.4	Improper Restriction of Rendered UI Layers or Frames in GitHub repository cockpit-hq/cockpit prior to 2.3.9-dev. **CVE ID : CVE-2023-0780**	https://hunter.dev/bounties/801efd0b-404b-4670-961a-12a986252fa4, https://github.com/cockpit-hq/cockpit/commit/8450bdf7e1dc23e9d88adf30a2aa9101c0c41720	A-AGE-COCK-270223/9
Vendor: akindo-sushiro					
Product: hong_kong_sushiro					
Affected Version(s): 3.0.3					
Insertion of Sensitive Information into Log File	13-Feb-2023	7.5	SUSHIRO App for Android outputs sensitive information to the log file, which may result in an attacker obtaining a credential information from the log file. Affected products/versions are	N/A	A-AKI-HONG-270223/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as follows: SUSHIRO Ver.4.0.31, Thailand SUSHIRO Ver.1.0.0, Hong Kong SUSHIRO Ver.3.0.2, Singapore SUSHIRO Ver.2.0.0, and Taiwan SUSHIRO Ver.2.0.1 **CVE ID : CVE-2023-22362**		
Product: singapore_sushiro					
Affected Version(s): 2.0.3					
Insertion of Sensitive Information into Log File	13-Feb-2023	7.5	SUSHIRO App for Android outputs sensitive information to the log file, which may result in an attacker obtaining a credential information from the log file. Affected products/versions are as follows: SUSHIRO Ver.4.0.31, Thailand SUSHIRO Ver.1.0.0, Hong Kong SUSHIRO Ver.3.0.2, Singapore SUSHIRO Ver.2.0.0, and Taiwan SUSHIRO Ver.2.0.1 **CVE ID : CVE-2023-22362**	N/A	A-AKI-SING-270223/11
Product: sushiro					
Affected Version(s): 4.0.31					
Insertion of Sensitive Information into Log File	13-Feb-2023	7.5	SUSHIRO App for Android outputs sensitive information to the log file, which may result in an attacker obtaining a credential information from the log file. Affected	N/A	A-AKI-SUSH-270223/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products/versions are as follows: SUSHIRO Ver.4.0.31, Thailand SUSHIRO Ver.1.0.0, Hong Kong SUSHIRO Ver.3.0.2, Singapore SUSHIRO Ver.2.0.0, and Taiwan SUSHIRO Ver.2.0.1 **CVE ID : CVE-2023-22362**		
Product: taiwan_sushiro					
Affected Version(s): 2.0.3					
Insertion of Sensitive Information into Log File	13-Feb-2023	7.5	SUSHIRO App for Android outputs sensitive information to the log file, which may result in an attacker obtaining a credential information from the log file. Affected products/versions are as follows: SUSHIRO Ver.4.0.31, Thailand SUSHIRO Ver.1.0.0, Hong Kong SUSHIRO Ver.3.0.2, Singapore SUSHIRO Ver.2.0.0, and Taiwan SUSHIRO Ver.2.0.1 **CVE ID : CVE-2023-22362**	N/A	A-AKI-TAIW-270223/13
Product: thailand_sushiro					
Affected Version(s): 2.0.3					
Insertion of Sensitive Information into Log File	13-Feb-2023	7.5	SUSHIRO App for Android outputs sensitive information to the log file, which may result in an attacker obtaining a credential information from the	N/A	A-AKI-THAI-270223/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			log file. Affected products/versions are as follows: SUSHIRO Ver.4.0.31, Thailand SUSHIRO Ver.1.0.0, Hong Kong SUSHIRO Ver.3.0.2, Singapore SUSHIRO Ver.2.0.0, and Taiwan SUSHIRO Ver.2.0.1 **CVE ID : CVE-2023-22362**		
Vendor: Amazon					
Product: opensearch					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.3.8					
Out-of-bounds Read	03-Feb-2023	4.3	OpenSearch Anomaly Detection identifies atypical data and receives automatic notifications. There is an issue with the application of document and field level restrictions in the Anomaly Detection plugin, where users with the Anomaly Detector role can read aggregated numerical data (e.g. averages, sums) of fields that are otherwise restricted to them. This issue only affects authenticated users who were previously granted read access to the indexes containing the restricted fields. This issue has been patched in versions 1.3.8 and 2.6.0. There are no	N/A	A-AMA-OPEN-270223/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workarounds for this issue. **CVE ID : CVE-2023-23933**		
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.6.0					
Out-of-bounds Read	03-Feb-2023	4.3	OpenSearch Anomaly Detection identifies atypical data and receives automatic notifications. There is an issue with the application of document and field level restrictions in the Anomaly Detection plugin, where users with the Anomaly Detector role can read aggregated numerical data (e.g. averages, sums) of fields that are otherwise restricted to them. This issue only affects authenticated users who were previously granted read access to the indexes containing the restricted fields. This issue has been patched in versions 1.3.8 and 2.6.0. There are no known workarounds for this issue. **CVE ID : CVE-2023-23933**	N/A	A-AMA-OPEN-270223/16
Vendor: amazonjs_project					
Product: amazonjs					
Affected Version(s): * Up to (including) 0.10					
Improper Neutralizat	13-Feb-2023	5.4	The Amazon JS WordPress plugin	N/A	A-AMA-AMAZ-270223/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			through 0.10 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0075**		
Vendor: Ampache					
Product: ampache					
Affected Version(s): * Up to (excluding) 5.5.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Feb-2023	8.8	SQL Injection in GitHub repository ampache/ampache prior to 5.5.7,develop. **CVE ID : CVE-2023-0771**	https://huntr.dev/bounties/2493f350-271b-4c38-9e1d-c8fa189c5ce1, https://github.com/ampache/ampache/commit/c456e66ef6fd8d11390181a40c66910ae01fbf4c	A-AMP-AMPA-270223/18
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Feb-2023	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository ampache/ampache prior to 5.5.7. **CVE ID : CVE-2023-0606**	https://github.com/ampache/ampache/commit/d3191503ca856dfe0b33d7cb17717ffd480046cb, https://huntr.dev/bounti	A-AMP-AMPA-270223/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				es/0bfed46d-ac96-43c4-93fb-13f68b4e711b	
Vendor: anchore					
Product: syft					
Affected Version(s): * Up to (excluding) 0.70.0					
Insertion of Sensitive Information into Log File	07-Feb-2023	7.5	syft is a a CLI tool and Go library for generating a Software Bill of Materials (SBOM) from container images and filesystems. A password disclosure flaw was found in Syft versions v0.69.0 and v0.69.1. This flaw leaks the password stored in the SYFT_ATTEST_PASSWORD environment variable. The `SYFT_ATTEST_PASSWORD` environment variable is for the `syft attest` command to generate attested SBOMs for the given container image. This environment variable is used to decrypt the private key (provided with `syft attest --key <path-to-key-file>`) during the signing process while generating an SBOM attestation. This vulnerability affects users running syft that have the `SYFT_ATTEST_PASSW	https://github.com/anchore/syft/commit/9995950c70e849f9921919faffbfcf46401f71f3, https://github.com/anchore/syft/security/advisories/GHSA-jp7v-3587-2956	A-ANC-SYFT-270223/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ORD` environment variable set with credentials (regardless of if the attest command is being used or not). Users that do not have the environment variable `SYFT_ATTEST_PASSWORD` set are not affected by this issue. The credentials are leaked in two ways: in the syft logs when `-vv` or `-vvv` are used in the syft command (which is any log level >= `DEBUG`) and in the attestation or SBOM only when the `syft-json` format is used. Note that as of v0.69.0 any generated attestations by the `syft attest` command are uploaded to the OCI registry (if you have write access to that registry) in the same way `cosign attach` is done. This means that any attestations generated for the affected versions of syft when the `SYFT_ATTEST_PASSWORD` environment variable was set would leak credentials in the attestation payload uploaded to the OCI registry. This issue has been patched in commit `9995950c70` and has		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been released as v0.70.0. There are no workarounds for this vulnerability. Users are advised to upgrade. **CVE ID : CVE-2023-24827**		
Vendor: answer					
Product: answer					
Affected Version(s): * Up to (excluding) 1.0.4					
N/A	08-Feb-2023	9.8	Improper Access Control in GitHub repository answerdev/answer prior to 1.0.4. **CVE ID : CVE-2023-0744**	https://huntr.dev/bounties/35a0e12f-1d54-4fc0-8779-6a4949b7c434, https://github.com/answerdev/answer/commit/c1fa2b13f6b547b96da60b23350bbe2b29de542d	A-ANS-ANSW-270223/21
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-2023	9	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.4. **CVE ID : CVE-2023-0740**	https://huntr.dev/bounties/802ee76d-fe01-482b-a9a4-34699a7c9110, https://github.com/answerdev/answer/commit/c3001de52af91f09c96e701facbce0b9fa0c98ad	A-ANS-ANSW-270223/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-2023	9	Cross-site Scripting (XSS) - DOM in GitHub repository answerdev/answer prior to 1.0.4. **CVE ID : CVE-2023-0741**	https://huntr.dev/bounties/78233bfa-871d-45e1-815f-dee73e397809, https://github.com/answerdev/answer/commit/c3001de52af91f09c96e701facbce0b9fa0c98ad	A-ANS-ANSW-270223/23
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-2023	9	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.4. **CVE ID : CVE-2023-0742**	https://huntr.dev/bounties/d73a2c03-7035-453b-9c04-c733ace65544, https://github.com/answerdev/answer/commit/c3001de52af91f09c96e701facbce0b9fa0c98ad	A-ANS-ANSW-270223/24
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-2023	9	Cross-site Scripting (XSS) - Generic in GitHub repository answerdev/answer prior to 1.0.4. **CVE ID : CVE-2023-0743**	https://github.com/answerdev/answer/commit/860b1a3bd8cfaa8827e6e6f50ab1d98fa4c2c816, https://huntr.dev/bounties/366cf8bb-19f6-4388-b089-	A-ANS-ANSW-270223/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				d0a260efd863	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Feb-2023	6.8	Race Condition in Switch in GitHub repository answerdev/answer prior to 1.0.4. **CVE ID : CVE-2023-0739**	https://huntr.dev/bounties/93d7fac9-50be-4624-9096-45b89fbfd4ae, https://github.com/answerdev/answer/commit/1ee34b884b905d14d4db457563176b77a974b992	A-ANS-ANSW-270223/26
Vendor: Apache					
Product: inlong					
Affected Version(s): From (including) 1.1.0 Up to (including) 1.5.0					
Deserialization of Untrusted Data	01-Feb-2023	9.8	Deserialization of Untrusted Data vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.1.0 through 1.5.0. Users are advised to upgrade to Apache InLong's latest version or cherry-pick https://github.com/apache/inlong/pull/7223 https://github.com/apache/inlong/pull/7223 to solve it. **CVE ID : CVE-2023-24997**	https://lists.apache.org/thread/nxvtxq7oxhwyzo9ty2hqz8rvh5r7ngd8	A-APA-INLO-270223/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Feb-2023	7.5	Out-of-bounds Read vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.1.0 through 1.5.0. Users are advised to upgrade to Apache InLong's latest version or cherry-pick https://github.com/apache/inlong/pull/7214 https://github.com/apache/inlong/pull/7214 to solve it. **CVE ID : CVE-2023-24977**	https://lists.apache.org/thread/ggozxorctn3tdll7bgmpwwcbjnd0s6w7	A-APA-INLO-270223/28
Product: kafka					
Affected Version(s): From (including) 2.3.0 Up to (including) 3.3.2					
Deserialization of Untrusted Data	07-Feb-2023	8.8	A possible security vulnerability has been identified in Apache Kafka Connect. This requires access to a Kafka Connect worker, and the ability to create/modify connectors on it with an arbitrary Kafka client SASL JAAS config and a SASL-based security protocol, which has been possible on Kafka Connect clusters since Apache Kafka 2.3.0. When configuring the connector via the Kafka Connect REST API, an authenticated operator can set the `sasl.jaas.config` property for any of the connector's Kafka	https://kafka.apache.org/cve-list	A-APA-KAFK-270223/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clients to "com.sun.security.auth.module.JndiLoginModule", which can be done via the `producer.override.sasl.jaas.config`, `consumer.override.sasl.jaas.config`, or `admin.override.sasl.jaas.config` properties. This will allow the server to connect to the attacker's LDAP server and deserialize the LDAP response, which the attacker can use to execute java deserialization gadget chains on the Kafka connect server. Attacker can cause unrestricted deserialization of untrusted data (or) RCE vulnerability when there are gadgets in the classpath. Since Apache Kafka 3.0.0, users are allowed to specify these properties in connector configurations for Kafka Connect clusters running with out-of-the-box configurations. Before Apache Kafka 3.0.0, users may not specify these properties unless the Kafka Connect cluster has been reconfigured with a connector client override policy that permits them. Since		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Apache Kafka 3.4.0, we have added a system property ("-Dorg.apache.kafka.disallowed.login.modules") to disable the problematic login modules usage in SASL JAAS configuration. Also by default "com.sun.security.auth.module.JndiLoginModule" is disabled in Apache Kafka 3.4.0. We advise the Kafka Connect users to validate connector configurations and only allow trusted JNDI configurations. Also examine connector dependencies for vulnerable versions and either upgrade their connectors, upgrading that specific dependency, or removing the connectors as options for remediation. Finally, in addition to leveraging the "org.apache.kafka.disallowed.login.modules" system property, Kafka Connect users can also implement their own connector client config override policy, which can be used to control which Kafka client properties can be overridden directly in a connector config and which cannot.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25194		
Product: nifi					
Affected Version(s): From (including) 1.2.0 Up to (including) 1.19.1					
Improper Restriction of XML External Entity Reference	10-Feb-2023	7.5	The ExtractCCDAAttributes Processor in Apache NiFi 1.2.0 through 1.19.1 does not restrict XML External Entity references. Flow configurations that include the ExtractCCDAAttributes Processor are vulnerable to malicious XML documents that contain Document Type Declarations with XML External Entity references. The resolution disables Document Type Declarations and disallows XML External Entity resolution in the ExtractCCDAAttributes Processor. **CVE ID : CVE-2023-22832**	https://lists.apache.org/thread/b51qs6y7b7r58vovddkv6wc16g2xbl3w, https://nifi.apache.org/security.html#CVE-2023-22832	A-APA-NIFI-270223/30
Product: sling_cms					
Affected Version(s): * Up to (excluding) 1.1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Feb-2023	6.1	An improper neutralization of input during web page generation ('Cross-site Scripting') [CWE-79] vulnerability in Sling App CMS version 1.1.4 and prior may allow an authenticated remote attacker to perform a	https://sling.apache.org/news.html	A-APA-SLIN-270223/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reflected cross-site scripting (XSS) attack in multiple features. Upgrade to Apache Sling App CMS >= 1.1.6 **CVE ID : CVE-2023-22849**		
Product: sling_jcr_base					
Affected Version(s): From (including) 2.0.6 Up to (excluding) 3.1.12					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	14-Feb-2023	7.5	Apache Sling JCR Base < 3.1.12 has a critical injection vulnerability when running on old JDK versions (JDK 1.8.191 or earlier) through utility functions in RepositoryAccessor. The functions getRepository and getRepositoryFromURL allow an application to access data stored in a remote location via JDNI and RMI. Users of Apache Sling JCR Base are recommended to upgrade to Apache Sling JCR Base 3.1.12 or later, or to run on a more recent JDK. **CVE ID : CVE-2023-25141**	https://sling.apache.org/news.html	A-APA-SLIN-270223/32
Vendor: art_gallery_management_system_project					
Product: art_gallery_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements	10-Feb-2023	9.8	Art Gallery Management System Project v1.0 was discovered to contain a SQL injection	N/A	A-ART-ART_-270223/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			vulnerability via the cid parameter at product.php. **CVE ID : CVE-2023-23162**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Feb-2023	9.8	Art Gallery Management System Project v1.0 was discovered to contain a SQL injection vulnerability via the editid parameter. **CVE ID : CVE-2023-23163**	N/A	A-ART-ART_-270223/34
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Feb-2023	6.1	A reflected cross-site scripting (XSS) vulnerability in Art Gallery Management System Project v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the artname parameter under ART TYPE option in the navigation bar. **CVE ID : CVE-2023-23161**	N/A	A-ART-ART_-270223/35
Vendor: Atlassian					
Product: jira_service_management					
Affected Version(s): 5.5.0					
Improper Authentication	01-Feb-2023	9.1	An authentication vulnerability was discovered in Jira Service Management Server and Data Center which allows an attacker to impersonate another user and gain	https://jira.atlassian.com/browse/JSDSERVER-12312	A-ATL-JIRA-270223/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to a Jira Service Management instance under certain circumstances_._ With write access to a User Directory and outgoing email enabled on a Jira Service Management instance, an attacker could gain access to signup tokens sent to users with accounts that have never been logged into. Access to these tokens can be obtained in two cases: * If the attacker is included on Jira issues or requests with these users, or * If the attacker is forwarded or otherwise gains access to emails containing a “View Request” link from these users. Bot accounts are particularly susceptible to this scenario. On instances with single sign-on, external customer accounts can be affected in projects where anyone can create their own account. **CVE ID : CVE-2023-22501**		
Affected Version(s): From (including) 5.3.0 Up to (excluding) 5.3.3					
Improper Authentication	01-Feb-2023	9.1	An authentication vulnerability was discovered in Jira Service Management	https://jira.atlassian.com/browse/J	A-ATL-JIRA-270223/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server and Data Center which allows an attacker to impersonate another user and gain access to a Jira Service Management instance under certain circumstances_._ With write access to a User Directory and outgoing email enabled on a Jira Service Management instance, an attacker could gain access to signup tokens sent to users with accounts that have never been logged into. Access to these tokens can be obtained in two cases: * If the attacker is included on Jira issues or requests with these users, or * If the attacker is forwarded or otherwise gains access to emails containing a “View Request” link from these users. Bot accounts are particularly susceptible to this scenario. On instances with single sign-on, external customer accounts can be affected in projects where anyone can create their own account. **CVE ID : CVE-2023-22501**	SDSERVER-12312	
Affected Version(s): From (including) 5.4.0 Up to (excluding) 5.4.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	01-Feb-2023	9.1	An authentication vulnerability was discovered in Jira Service Management Server and Data Center which allows an attacker to impersonate another user and gain access to a Jira Service Management instance under certain circumstances_._ With write access to a User Directory and outgoing email enabled on a Jira Service Management instance, an attacker could gain access to signup tokens sent to users with accounts that have never been logged into. Access to these tokens can be obtained in two cases: * If the attacker is included on Jira issues or requests with these users, or * If the attacker is forwarded or otherwise gains access to emails containing a “View Request” link from these users. Bot accounts are particularly susceptible to this scenario. On instances with single sign-on, external customer accounts can be affected in projects where anyone can create their own account.	https://jira.atlassian.com/browse/JSDSERVER-12312	A-ATL-JIRA-270223/38

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22501		
Vendor: best_online_news_portal_project					
Product: best_online_news_portal					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Feb-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Best Online News Portal 1.0. Affected is an unknown function of the component Login Page. The manipulation of the argument username leads to sql injection. 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-220644. **CVE ID : CVE-2023-0784**	N/A	A-BES-BEST-270223/39
Exposure of Sensitive Information Through Data Queries	12-Feb-2023	5.3	A vulnerability classified as problematic was found in SourceCodester Best Online News Portal 1.0. Affected by this vulnerability is an unknown functionality of the file check_availability.php. The manipulation of the argument username leads to exposure of sensitive information through data queries. The attack can be	N/A	A-BES-BEST-270223/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-220645 was assigned to this vulnerability. **CVE ID : CVE-2023-0785**		
Vendor: bgerp					
Product: bgerp					
Affected Version(s): 22.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	6.1	bgERP v22.31 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the Search parameter. **CVE ID : CVE-2023-25241**	N/A	A-BGE-BGER-270223/41
Vendor: bplugins					
Product: html5_audio_player					
Affected Version(s): * Up to (excluding) 2.1.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The Html5 Audio Player WordPress plugin before 2.1.12 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0170**	N/A	A-BPL-HTML-270223/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Brave					
Product: adblock-lists					
Affected Version(s): * Up to (excluding) 2022-05-25					
URL Redirection to Untrusted Site ('Open Redirect')	09-Feb-2023	6.1	Prior to commit 51867e0d15a6d7f80d5b714fd0e9976b9c160bb0, https://github.com/brave/adblock-lists removed redirect interceptors on some websites like Facebook in which the redirect interceptor may have been there for security purposes. This could potentially cause open redirects on these websites. Brave's redirect interceptor removal feature is known as "debouncing" and is intended to remove unnecessary redirects that track users across the web. **CVE ID : CVE-2023-22798**	https://hackerone.com/reports/1579374	A-BRA-ADBL-270223/43
Vendor: btcpayserver					
Product: btcpayserver					
Affected Version(s): * Up to (excluding) 1.7.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository btcpayserver/btcpayserver prior to 1.7.11. **CVE ID : CVE-2023-0810**	https://hunter.dev/bounties/a48414ea-63d9-453c-b3f3-2c927b71ec68, https://github.com/btcpayserver/btc	A-BTC-BTCP-270223/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				payserver/commit/dffa6accb04df7b80bc584dedef22c9297292ce6	
Affected Version(s): * Up to (excluding) 1.7.6					
URL Redirection to Untrusted Site ('Open Redirect')	08-Feb-2023	6.1	Open Redirect in GitHub repository btcpayserver/btcpayserver prior to 1.7.6. **CVE ID : CVE-2023-0748**	https://github.com/btcpayserver/btcpayserver/commit/c2cfa17e9619046b43987627b8429541d2834109, https://huntr.dev/bounties/1a0403b6-9ec9-4587-b559-b1afba798c86	A-BTC-BTCP-270223/45
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository btcpayserver/btcpayserver prior to 1.7.6. **CVE ID : CVE-2023-0747**	https://github.com/btcpayserver/btcpayserver/commit/d4e464ad4ef0cbbf61751e70f77865de325dd6cf, https://huntr.dev/bounties/7830b9b4-af2e-44ef-8b00-ee2491d4e7ff	A-BTC-BTCP-270223/46
Vendor: butterfly-button_project					
Product: butterfly-button					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	15-Feb-2023	4.6	Butterfly Button plugin may leave traces of its use on user's device. Since it is used for reporting domestic problems, this may lead to spouse knowing about its use. **CVE ID : CVE-2023-24499**	N/A	A-BUT-BUTT-270223/47
Vendor: calendar_event_management_system_project					
Product: calendar_event_management_system					
Affected Version(s): 2.3.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Feb-2023	9.8	A vulnerability was found in Calendar Event Management System 2.3.0. It has been rated as critical. This issue affects some unknown processing of the component Login Page. The manipulation of the argument name/pwd leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-220175. **CVE ID : CVE-2023-0663**	N/A	A-CAL-CALE-270223/48
Improper Neutralization of Special Elements used in an SQL Command	04-Feb-2023	8.8	A vulnerability, which was classified as critical, was found in Calendar Event Management System 2.3.0. This affects an unknown part. The manipulation of the	N/A	A-CAL-CALE-270223/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			argument start/end 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 identifier VDB-220197 was assigned to this vulnerability. **CVE ID : CVE-2023-0675**		
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')	06-Feb-2023	9.8	A vulnerability was found in SourceCodester Canteen Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file removeUser.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-220220. **CVE ID : CVE-2023-0679**	N/A	A-CAN-CANT-270223/50
Improper Neutralization of Special Elements	11-Feb-2023	9.8	A vulnerability was found in SourceCodester Canteen Management System 1.0. It has been	N/A	A-CAN-CANT-270223/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			declared as critical. This vulnerability affects the function query of the file removeOrder.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. The identifier of this vulnerability is VDB-220624. **CVE ID : CVE-2023-0781**		
Vendor: caphyon					
Product: advanced_installer					
Affected Version(s): * Up to (including) 20.0					
N/A	08-Feb-2023	7.8	Privilege escalation in the MSI repair functionality in Caphyon Advanced Installer 20.0 and below allows attackers to access and manipulate system files. **CVE ID : CVE-2023-25396**	N/A	A-CAP-ADVA-270223/52
Vendor: chikoi_project					
Product: chikoi					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command	13-Feb-2023	9.8	ChiKoi v1.0 was discovered to contain a SQL injection vulnerability via the load_file function. **CVE ID : CVE-2023-24084**	N/A	A-CHI-CHIK-270223/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')					
Vendor: churchcrm					
Product: churchcrm					
Affected Version(s): * Up to (including) 4.5.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Feb-2023	7.2	ChurchCRM v4.5.3 and below was discovered to contain a SQL injection vulnerability via the EID parameter at GetText.php. **CVE ID : CVE-2023-24684**	N/A	A-CHU-CHUR-270223/54
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Feb-2023	7.2	ChurchCRM v4.5.3 and below was discovered to contain a SQL injection vulnerability via the Event parameter under the Event Attendance reports module. **CVE ID : CVE-2023-24685**	N/A	A-CHU-CHUR-270223/55
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Feb-2023	5.4	ChurchCRM 4.5.3 and below was discovered to contain a stored cross-site scripting (XSS) vulnerability at /api/public/register/family. **CVE ID : CVE-2023-24690**	N/A	A-CHU-CHUR-270223/56
Improper Neutralization of Input During Web Page Generation	09-Feb-2023	4.8	An issue in the CSV Import function of ChurchCRM v4.5.3 and below allows attackers to execute arbitrary code via importing a crafted CSV file.	N/A	A-CHU-CHUR-270223/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-24686**		
Vendor: Cisco					
Product: iox					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	A-CIS-IOX-270223/58
Vendor: cloak_front_end_email_project					
Product: cloak_front_end_email					
Affected Version(s): * Up to (including) 1.9.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The Cloak Front End Email WordPress plugin through 1.9.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0150**	N/A	A-CLO-CLOA-270223/59
Vendor: clockwork_web_project					
Product: clockwork_web					
Affected Version(s): * Up to (excluding) 0.1.2					
Cross-Site Request Forgery (CSRF)	02-Feb-2023	6.5	Clockwork Web before 0.1.2, when Rails before 5.2 is used, allows CSRF. **CVE ID : CVE-2023-25015**	https://github.com/ankane/clockwork_web/commit/ec2896503ee231588547c2fad4cb93a94e78f857, https://github.com/ankane/clockwork_web/issues/4, https://github.com/ankane/clockwork_web/compare/v0.1.1...v0.1.2	A-CLO-CLOC-270223/60
Vendor: cncf					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: opentelemetry-go_contrib					
Affected Version(s): 0.38.0					
Uncontrolled Resource Consumption	08-Feb-2023	7.5	opentelemetry-go-contrib is a collection of extensions for OpenTelemetry-Go. The v0.38.0 release of `go.opentelemetry.io/contrib/instrumentation/net/http/otelhttp` uses the `httpconv.ServerRequest` function to annotate metric measurements for the `http.server.request_content_length`, `http.server.response_content_length`, and `http.server.duration` instruments. The `ServerRequest` function sets the `http.target` attribute value to be the whole request URI (including the query string)[^1]. The metric instruments do not "forget" previous measurement attributes when `cumulative` temporality is used, this means the cardinality of the measurements allocated is directly correlated with the unique URIs handled. If the query string is constantly random, this will result in a constant increase in memory allocation that can be	https://github.com/open-telemetry/opentelemetry-go/blob/v1.12.0/semconv/internal/v2/http.go#L159, https://github.com/open-telemetry/opentelemetry-go-contrib/security/advisories/GHSA-5r5m-65gx-7vrh	A-CNC-OPEN-270223/61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used in a denial-of-service attack. This issue has been addressed in version 0.39.0. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-25151**		
Vendor: connectwise					
Product: automate					
Affected Version(s): 2022.11					
Improper Restriction of Rendered UI Layers or Frames	01-Feb-2023	6.1	** DISPUTED ** Connectwise Automate 2022.11 is vulnerable to Clickjacking. The login screen can be iframed and used to manipulate users to perform unintended actions. NOTE: the vendor's position is that a Content-Security-Policy HTTP response header is present to block this attack. **CVE ID : CVE-2023-23126**	N/A	A-CON-AUTO-270223/62
Cleartext Transmission of Sensitive Information	01-Feb-2023	5.9	** DISPUTED ** Connectwise Automate 2022.11 is vulnerable to Cleartext authentication. Authentication is being done via HTTP (cleartext) with SSL disabled. OTE: the vendor's position is that, by design, this is controlled by a	N/A	A-CON-AUTO-270223/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration option in which a customer can choose to use HTTP (rather than HTTPS) during troubleshooting. **CVE ID : CVE-2023-23130**		
Product: connectwise					
Affected Version(s): 22.8.10013.8329					
N/A	01-Feb-2023	6.1	** DISPUTED **Connectwise Control 22.8.10013.8329 is vulnerable to Cross Origin Resource Sharing (CORS). The vendor's position is that two endpoints have Access-Control-Allow-Origin wildcarding to support product functionality, and that there is no risk from this behavior. The vulnerability report is thus not valid. **CVE ID : CVE-2023-23128**	N/A	A-CON-CONN-270223/64
Missing Encryption of Sensitive Data	01-Feb-2023	5.3	** DISPUTED **In Connectwise Control 22.8.10013.8329, the login page does not implement HSTS headers therefore not enforcing HTTPS. NOTE: the vendor's position is that, by design, this is controlled by a configuration option in which a customer can choose to use HTTP	N/A	A-CON-CONN-270223/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(rather than HTTPS) during troubleshooting. **CVE ID : CVE-2023-23127**		
Product: control					
Affected Version(s): * Up to (excluding) 22.9.10032					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	13-Feb-2023	8.8	ConnectWise Control before 22.9.10032 (formerly known as ScreenConnect) fails to validate user-supplied parameters such as the Bin/ConnectWiseControl.Client.exe h parameter. This results in reflected data and injection of malicious code into a downloaded executable. The executable can be used to execute malicious queries or as a denial-of-service vector. **CVE ID : CVE-2023-25719**	N/A	A-CON-CONT-270223/66
Affected Version(s): * Up to (including) 22.9.10032					
Improper Verification of Cryptographic Signature	13-Feb-2023	9.8	The cryptographic code signing process and controls on ConnectWise Control through 22.9.10032 (formerly known as ScreenConnect) are cryptographically flawed. An attacker can remotely generate or locally alter file contents and bypass code-signing controls. This can be used to execute code as a trusted application	N/A	A-CON-CONT-270223/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provider, escalate privileges, or execute arbitrary commands in the context of the user. The attacker tampers with a trusted, signed executable in transit. **CVE ID : CVE-2023-25718**		
Vendor: couchbase					
Product: couchbase_server					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 6.6.6					
Cleartext Transmission of Sensitive Information	06-Feb-2023	7.5	Couchbase Server before 6.6.6, 7.x before 7.0.5, and 7.1.x before 7.1.2 exposes Sensitive Information to an Unauthorized Actor. **CVE ID : CVE-2023-25016**	https://www.couchbase.com/alerts/	A-COU-COUC-270223/68
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.5					
Cleartext Transmission of Sensitive Information	06-Feb-2023	7.5	Couchbase Server before 6.6.6, 7.x before 7.0.5, and 7.1.x before 7.1.2 exposes Sensitive Information to an Unauthorized Actor. **CVE ID : CVE-2023-25016**	https://www.couchbase.com/alerts/	A-COU-COUC-270223/69
Affected Version(s): From (including) 7.1.0 Up to (excluding) 7.1.2					
Cleartext Transmission of Sensitive Information	06-Feb-2023	7.5	Couchbase Server before 6.6.6, 7.x before 7.0.5, and 7.1.x before 7.1.2 exposes Sensitive Information to an Unauthorized Actor. **CVE ID : CVE-2023-25016**	https://www.couchbase.com/alerts/	A-COU-COUC-270223/70
Vendor: cozmoslabs					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: profile_builder					
Affected Version(s): * Up to (including) 3.9.0					
Incorrect Authorization	14-Feb-2023	6.5	The Profile Builder – User Profile & User Registration Forms plugin for WordPress is vulnerable to sensitive information disclosure via the [user_meta] shortcode in versions up to, and including 3.9.0. This is due to insufficient restriction on sensitive user meta values that can be called via that shortcode. This makes it possible for authenticated attackers, with subscriber-level permissions, and above to retrieve sensitive user meta that can be used to gain access to a high privileged user account. This does require the Usermeta shortcode be enabled to be exploited. **CVE ID : CVE-2023-0814**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2864329%40profile-builder&new=2864329%40profile-builder&sfp_email=&sfph_mail=	A-COZ-PROF-270223/71
Vendor: crocoblock					
Product: jetwidgets_for_elementor					
Affected Version(s): * Up to (including) 1.0.13					
Improper Neutralization of Input During Web Page Generation	13-Feb-2023	5.4	The JetWidgets For Elementor WordPress plugin through 1.0.13 does not validate and escape some of its shortcode attributes before outputting them back in a page/post	N/A	A-CRO-JETW-270223/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0034**		
Vendor: cryptography_project					
Product: cryptography					
Affected Version(s): From (including) 1.8 Up to (excluding) 39.0.1					
Improper Check for Unusual or Exceptional Conditions	07-Feb-2023	6.5	cryptography is a package designed to expose cryptographic primitives and recipes to Python developers. In affected versions `Cipher.update_into` would accept Python objects which implement the buffer protocol, but provide only immutable buffers. This would allow immutable objects (such as `bytes`) to be mutated, thus violating fundamental rules of Python and resulting in corrupted output. This now correctly raises an exception. This issue has been present since `update_into` was originally introduced in cryptography 1.8. **CVE ID : CVE-2023-23931**	https://github.com/pyca/cryptography/security/advisories/GHSA-w7pp-m8wf-vj6r, https://github.com/pyca/cryptography/pull/8230/commits/94a50a9731f35405f0357fa5f3b177d46a726ab3	A-CRY-CRYP-270223/73
Vendor: cusrev					
Product: customer_reviews_for_woocommerce					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 5.16.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Feb-2023	8.8	The Customer Reviews for WooCommerce WordPress plugin before 5.16.0 does not validate one of its shortcode attribute, which could allow users with a contributor role and above to include arbitrary files via a traversal attack. This could also allow them to read non PHP files and retrieve their content. RCE could also be achieved if the attacker manage to upload a malicious image containing PHP code, and then include it via the affected attribute, on a default WP install, authors could easily achieve that given that they have the upload_file capability. **CVE ID : CVE-2023-0080**	N/A	A-CUS-CUST-270223/74
Vendor: datahub_project					
Product: datahub					
Affected Version(s): * Up to (excluding) 0.8.45					
Improper Control of Dynamically-Managed Code Resources	11-Feb-2023	9.8	DataHub is an open-source metadata platform. The AuthServiceClient which is responsible for creation of new accounts, verifying credentials, resetting them or requesting	https://github.com/datahub-project/datahub/security/advisories/GHSA-6rpf-5cfg-h8f3	A-DAT-DATA-270223/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access tokens, crafts multiple JSON strings using format strings with user-controlled data. This means that an attacker may be able to augment these JSON strings to be sent to the backend and that can potentially be abused by including new or colliding values. This issue may lead to an authentication bypass and the creation of system accounts, which effectively can lead to full system compromise. Users are advised to upgrade. There are no known workarounds for this vulnerability. This vulnerability was discovered and reported by the GitHub Security lab and is tracked as GHSL-2022-080. **CVE ID : CVE-2023-25560**		
Improper Handling of Exceptional Conditions	11-Feb-2023	9.8	DataHub is an open-source metadata platform. In the event a system is using Java Authentication and Authorization Service (JAAS) authentication and that system is given a configuration which contains an error, the authentication for the system will fail open	https://github.com/datahub-project/datahub/security/advisories/GHSA-7wc6-p6c4-522c	A-DAT-DATA-270223/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and allow an attacker to login using any username and password. The reason for this is that while an error is thrown in the `authenticateJaasUser` method it is swallowed without propagating the error. As a result of this issue unauthenticated users may gain access to the system. Users are advised to upgrade. There are no known workarounds for this issue. This vulnerability was discovered and reported by the GitHub Security lab and is tracked as GHSL-2022-081. **CVE ID : CVE-2023-25561**		
Insufficient Session Expiration	11-Feb-2023	9.8	DataHub is an open-source metadata platform. In versions of DataHub prior to 0.8.45 Session cookies are only cleared on new sign-in events and not on logout events. Any authentication checks using the `AuthUtils.hasValidSessionCookie()` method could be bypassed by using a cookie from a logged out session, as a result any logged out session cookie may be accepted as valid and	https://github.com/datahub-project/datahub/security/advisories/GHSA-3974-hxjh-m3jj	A-DAT-DATA-270223/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			therefore lead to an authentication bypass to the system. Users are advised to upgrade. There are no known workarounds for this issue. This vulnerability was discovered and reported by the GitHub Security lab and is tracked as GHSL-2022-083. **CVE ID : CVE-2023-25562**		
Server-Side Request Forgery (SSRF)	11-Feb-2023	9.1	DataHub is an open-source metadata platform. The DataHub frontend acts as a proxy able to forward any REST or GraphQL requests to the backend. The goal of this proxy is to perform authentication if needed and forward HTTP requests to the DataHub Metadata Store (GMS). It has been discovered that the proxy does not adequately construct the URL when forwarding data to GMS, allowing external users to reroute requests from the DataHub Frontend to any arbitrary hosts. As a result attackers may be able to reroute a request from originating from the frontend proxy to any	https://github.com/datahub-project/datahub/security/advisories/GHSA-5w2h-q83m-65xg	A-DAT-DATA-270223/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other server and return the result. This vulnerability was discovered and reported by the GitHub Security lab and is tracked as GHSL-2022-076. **CVE ID : CVE-2023-25557**		
Incorrect Authorization	11-Feb-2023	8.1	DataHub is an open-source metadata platform. When not using authentication for the metadata service, which is the default configuration, the Metadata service (GMS) will use the X-DataHub-Actor HTTP header to infer the user the frontend is sending the request on behalf of. When the backends retrieves the header, its name is retrieved in a case-insensitive way. This case differential can be abused by an attacker to smuggle an X-DataHub-Actor header with different casing (eg: X-DATAHUB-ACTOR). This issue may lead to an authorization bypass by allowing any user to impersonate the system user account and perform any actions on its behalf. This vulnerability was discovered and	https://github.com/datahub-project/datahub/security/advisories/GHSA-qgp2-qr66-j8r8	A-DAT-DATA-270223/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reported by the GitHub Security lab and is tracked as GHSL-2022-079. **CVE ID : CVE-2023-25559**		
Affected Version(s): * Up to (excluding) 0.9.5					
Deserialization of Untrusted Data	11-Feb-2023	8.8	DataHub is an open-source metadata platform. When the DataHub frontend is configured to authenticate via SSO, it will leverage the pac4j library. The processing of the `id_token` is done in an unsafe manner which is not properly accounted for by the DataHub frontend. Specifically, if any of the id_token claims value start with the {#sb64} prefix, pac4j considers the value to be a serialized Java object and will deserialize it. This issue may lead to Remote Code Execution (RCE) in the worst case. Although a `RestrictedObjectInputStream` is in place, that puts some restriction on what classes can be deserialized, it still allows a broad range of java packages and potentially exploitable with different gadget chains. Users are advised to upgrade. There are no known	https://github.com/datahub-project/datahub/security/advisories/GHSA-hrwp-2q5c-86wv, https://github.com/datahub-project/datahub/commit/2a182f484677d056730d6b4e9f0143e67368359f	A-DAT-DATA-270223/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds. This vulnerability was discovered and reported by the GitHub Security lab and is tracked as GHSL-2022-086. **CVE ID : CVE-2023-25558**		
Vendor: Dell					
Product: alienware_command_center					
Affected Version(s): * Up to (including) 5.5.37.0					
Improper Input Validation	10-Feb-2023	7.8	Dell Alienware Command Center versions 5.5.37.0 and prior contain an Improper Input validation vulnerability. A local authenticated malicious user could potentially send malicious input to a named pipe in order to elevate privileges on the system. **CVE ID : CVE-2023-24569**	https://www.dell.com/support/kbdoc/en-us/000208327/dsa-2023-044	A-DEL-ALIE-270223/81
Product: alienware_update					
Affected Version(s): 4.6.0					
N/A	10-Feb-2023	7.1	Dell Command | Update, Dell Update, and Alienware Update versions before 4.6.0 and 4.7.1 contain Insecure Operation on Windows Junction in the installer component. A local malicious user may potentially exploit this	https://www.dell.com/support/kbdoc/en-us/000208038/dsa-2023-031	A-DEL-ALIE-270223/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability leading to arbitrary file delete. **CVE ID : CVE-2023-23698**		
Affected Version(s): 4.7.1					
N/A	10-Feb-2023	7.1	Dell Command | Update, Dell Update, and Alienware Update versions before 4.6.0 and 4.7.1 contain Insecure Operation on Windows Junction in the installer component. A local malicious user may potentially exploit this vulnerability leading to arbitrary file delete. **CVE ID : CVE-2023-23698**	https://www.dell.com/support/kbdoc/en-us/000208038/dsa-2023-031	A-DEL-ALIE-270223/83
Product: command_update					
Affected Version(s): 4.6.0					
N/A	10-Feb-2023	7.1	Dell Command | Update, Dell Update, and Alienware Update versions before 4.6.0 and 4.7.1 contain Insecure Operation on Windows Junction in the installer component. A local malicious user may potentially exploit this vulnerability leading to arbitrary file delete. **CVE ID : CVE-2023-23698**	https://www.dell.com/support/kbdoc/en-us/000208038/dsa-2023-031	A-DEL-COMM-270223/84
Affected Version(s): 4.7.1					
N/A	10-Feb-2023	7.1	Dell Command | Update, Dell Update, and Alienware Update	https://www.dell.com/support/kbdo	A-DEL-COMM-270223/85

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions before 4.6.0 and 4.7.1 contain Insecure Operation on Windows Junction in the installer component. A local malicious user may potentially exploit this vulnerability leading to arbitrary file delete. **CVE ID : CVE-2023-23698**	c/en-us/000208038/dsa-2023-031	
Product: command_|_integration_suite_for_system_center					
Affected Version(s): * Up to (excluding) 6.4.0					
Improper Link Resolution Before File Access ('Link Following')	13-Feb-2023	3.3	Dell Command | Integration Suite for System Center, versions before 6.4.0 contain an arbitrary folder delete vulnerability during uninstallation. A locally authenticated malicious user may potentially exploit this vulnerability leading to arbitrary folder deletion. **CVE ID : CVE-2023-24572**	https://www.dell.com/support/kbdoc/en-us/000207931/dsa-2023-032	A-DEL-COMM-270223/86
Product: command_|_intel_vpro_out_of_band					
Affected Version(s): * Up to (excluding) 4.4.0					
Incorrect Authorization	07-Feb-2023	7.8	Dell Command Intel vPro Out of Band, versions prior to 4.3.1, contain an Improper Authorization vulnerability. A locally authenticated malicious users could potentially exploit this vulnerability in order to	https://www.dell.com/support/kbdoc/en-us/000208331/dsa-2023-029-dell-command-intel-vpro-	A-DEL-COMM-270223/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write arbitrary files to the system. **CVE ID : CVE-2023-23696**	out-of-band-security-update-for-an-improper-authorization-vulnerability	
Improper Link Resolution Before File Access ('Link Following')	13-Feb-2023	3.3	Dell Command | Intel vPro Out of Band, versions before 4.4.0, contain an arbitrary folder delete vulnerability during uninstallation. A locally authenticated malicious user may potentially exploit this vulnerability leading to arbitrary folder deletion. **CVE ID : CVE-2023-23697**	https://www.dell.com/support/kbdoc/en-us/000207929/dsa-2023-030	A-DEL-COMM-270223/88
Product: command_|_monitor					
Affected Version(s): * Up to (excluding) 10.9					
N/A	10-Feb-2023	7.1	Dell Command | Monitor versions prior to 10.9 contain an arbitrary folder delete vulnerability during uninstallation. A locally authenticated malicious user may potentially exploit this vulnerability leading to arbitrary folder deletion. **CVE ID : CVE-2023-24573**	https://www.dell.com/support/kbdoc/en-us/000207973/dsa-2023-033	A-DEL-COMM-270223/89
Product: emc_networker					
Affected Version(s): * Up to (including) 19.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	03-Feb-2023	9.8	EMC NetWorker may potentially be vulnerable to an unauthenticated remote code execution vulnerability in the NetWorker Client execution service (nsrexecd) irrespective of any auth used. **CVE ID : CVE-2023-24576**	https://www.dell.com/support/kbdoc/en-us/000208258/dsa-2023-041-dell-networker-security-update-for-nsrdump-vulnerability	A-DEL-EMC_-270223/90
Affected Version(s): 19.7.0.2					
Improper Control of Generation of Code ('Code Injection')	03-Feb-2023	9.8	EMC NetWorker may potentially be vulnerable to an unauthenticated remote code execution vulnerability in the NetWorker Client execution service (nsrexecd) irrespective of any auth used. **CVE ID : CVE-2023-24576**	https://www.dell.com/support/kbdoc/en-us/000208258/dsa-2023-041-dell-networker-security-update-for-nsrdump-vulnerability	A-DEL-EMC_-270223/91
Vendor: deltaww					
Product: diascreen					
Affected Version(s): * Up to (including) 1.2.1.23					
Out-of-bounds Write	08-Feb-2023	7.8	Delta Electronics DIAScreen versions 1.2.1.23 and prior are vulnerable to out-of-bounds write, which may allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2023-0249**	N/A	A-DEL-DIAS-270223/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	08-Feb-2023	7.8	Delta Electronics DIAScreen versions 1.2.1.23 and prior are vulnerable to a stack-based buffer overflow, which could allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2023-0250**	N/A	A-DEL-DIAS-270223/93
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Feb-2023	7.8	Delta Electronics DIAScreen versions 1.2.1.23 and prior are vulnerable to a buffer overflow through improper restrictions of operations within memory, which could allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2023-0251**	N/A	A-DEL-DIAS-270223/94
Product: dopsoft					
Affected Version(s): * Up to (excluding) 4.00.16.22					
Out-of-bounds Write	03-Feb-2023	7.8	Delta Electronics DOPSoft versions 4.00.16.22 and prior are vulnerable to a stack-based buffer overflow, which could allow an attacker to remotely execute arbitrary code when a malformed file is introduced to the software. **CVE ID : CVE-2023-0123**	N/A	A-DEL-DOPS-270223/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Feb-2023	7.8	Delta Electronics DOPSoft versions 4.00.16.22 and prior are vulnerable to an out-of-bounds write, which could allow an attacker to remotely execute arbitrary code when a malformed file is introduced to the software. **CVE ID : CVE-2023-0124**	N/A	A-DEL-DOPS-270223/96
Vendor: devolutions					
Product: devolutions_server					
Affected Version(s): From (including) 2022.3.1 Up to (including) 2022.3.9					
N/A	12-Feb-2023	6.5	Improper access control in Devolutions Server allows an authenticated user to access unauthorized sensitive data. **CVE ID : CVE-2023-0661**	https://devolutions.net/security/advisories/DEVO-2023-0002	A-DEV-DEVO-270223/97
Vendor: devowl					
Product: wordpress_real_media_library					
Affected Version(s): * Up to (including) 4.18.28					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Feb-2023	5.4	The Real Media Library: Media Library Folder & File Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via folder names in versions up to, and including, 4.18.28 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers	https://devowlio.gitbook.io/changelogs/wordpress-plugins/real-media-library	A-DEV-WORD-270223/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with author-level permissions and above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-0253**		
Vendor: discourse					
Product: discourse					
Affected Version(s): 2.3.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/99
Affected Version(s): * Up to (excluding) 3.0.1					
N/A	08-Feb-2023	5.7	Discourse is an open source discussion platform. In affected versions a malicious user can cause a regular expression denial of service using a carefully crafted git URL. This issue is patched in the	https://github.com/discourse/discourse/commit/ec4c30270887366dc28788bc4ab8a22a098573cd,	A-DIS-DISC-270223/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			latest stable, beta and tests-passed versions of Discourse. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-25167**	https://github.com/discourse/discourse/security/advisories/GHSA-4w55-w26q-r35w	
Affected Version(s): * Up to (including) 3.0.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/101
Affected Version(s): 1.1.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of	N/A	A-DIS-DISC-270223/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**		
Affected Version(s): 1.2.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/103
Affected Version(s): 1.3.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable	N/A	A-DIS-DISC-270223/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**		
Affected Version(s): 1.4.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/105
Affected Version(s): 1.5.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments	N/A	A-DIS-DISC-270223/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**		
Affected Version(s): 1.6.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/107
Affected Version(s): 1.7.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts.	N/A	A-DIS-DISC-270223/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23615		
Affected Version(s): 1.8.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/109
Affected Version(s): 1.9.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.0.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/111
Affected Version(s): 2.1.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/112
Affected Version(s): 2.2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/113
Affected Version(s): 2.4.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/114
Affected Version(s): 2.5.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/115
Affected Version(s): 2.6.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/116
Affected Version(s): 2.7.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/117
Affected Version(s): 2.8.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/118
Affected Version(s): 2.9.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/119
Affected Version(s): 3.0.0					
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/120
Affected Version(s): 3.1.0					
N/A	08-Feb-2023	5.7	Discourse is an open source discussion	https://github.com/disc	A-DIS-DISC-270223/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			platform. In affected versions a malicious user can cause a regular expression denial of service using a carefully crafted git URL. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-25167**	ourse/discourse/commit/ec4c30270887366dc28788bc4ab8a22a098573cd, https://github.com/discourse/discourse/security/advisories/GHSA-4w55-w26q-r35w	
Improper Access Control	03-Feb-2023	5.3	Discourse is an open source discussion platform. The embeddable comments can be exploited to create new topics as any user but without any clear title or content. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. As a workaround, disable embeddable comments by deleting all embeddable hosts. **CVE ID : CVE-2023-23615**	N/A	A-DIS-DISC-270223/122
Vendor: Djangoproject					
Product: django					
Affected Version(s): From (including) 3.2 Up to (excluding) 3.2.17					
Allocation of Resources Without	01-Feb-2023	7.5	In Django 3.2 before 3.2.17, 4.0 before 4.0.9, and 4.1 before 4.1.6, the parsed values of	https://docs.djangoproject.com/en/4.1/releases/s	A-DJA-DJAN-270223/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			Accept-Language headers are cached in order to avoid repetitive parsing. This leads to a potential denial-of-service vector via excessive memory usage if the raw value of Accept-Language headers is very large. **CVE ID : CVE-2023-23969**	ecurity/, https://www.djangoproject.com/weblog/2023/feb/01/security-releases/	
Affected Version(s): From (including) 3.2 Up to (excluding) 3.2.18					
Uncontrolled Resource Consumption	15-Feb-2023	7.5	An issue was discovered in the Multipart Request Parser in Django 3.2 before 3.2.18, 4.0 before 4.0.10, and 4.1 before 4.1.7. Passing certain inputs (e.g., an excessive number of parts) to multipart forms could result in too many open files or memory exhaustion, and provided a potential vector for a denial-of-service attack. **CVE ID : CVE-2023-24580**	https://docs.djangoproject.com/en/4.1/releases/security/, https://www.djangoproject.com/weblog/2023/feb/14/security-releases/	A-DJA-DJAN-270223/124
Affected Version(s): From (including) 4.0 Up to (excluding) 4.0.10					
Uncontrolled Resource Consumption	15-Feb-2023	7.5	An issue was discovered in the Multipart Request Parser in Django 3.2 before 3.2.18, 4.0 before 4.0.10, and 4.1 before 4.1.7. Passing certain inputs (e.g., an excessive number of parts) to multipart	https://docs.djangoproject.com/en/4.1/releases/security/, https://www.djangoproject.com/weblog/2023/f	A-DJA-DJAN-270223/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			forms could result in too many open files or memory exhaustion, and provided a potential vector for a denial-of-service attack. **CVE ID : CVE-2023-24580**	eb/14/security-releases/	
Affected Version(s): From (including) 4.0 Up to (excluding) 4.0.9					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In Django 3.2 before 3.2.17, 4.0 before 4.0.9, and 4.1 before 4.1.6, the parsed values of Accept-Language headers are cached in order to avoid repetitive parsing. This leads to a potential denial-of-service vector via excessive memory usage if the raw value of Accept-Language headers is very large. **CVE ID : CVE-2023-23969**	https://docs.djangoproject.com/en/4.1/releases/security/, https://www.djangoproject.com/weblog/2023/feb/01/security-releases/	A-DJA-DJAN-270223/126
Affected Version(s): From (including) 4.1 Up to (excluding) 4.1.6					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In Django 3.2 before 3.2.17, 4.0 before 4.0.9, and 4.1 before 4.1.6, the parsed values of Accept-Language headers are cached in order to avoid repetitive parsing. This leads to a potential denial-of-service vector via excessive memory usage if the raw value of Accept-Language headers is very large.	https://docs.djangoproject.com/en/4.1/releases/security/, https://www.djangoproject.com/weblog/2023/feb/01/security-releases/	A-DJA-DJAN-270223/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23969		
Affected Version(s): From (including) 4.1 Up to (excluding) 4.1.7					
Uncontrolled Resource Consumption	15-Feb-2023	7.5	An issue was discovered in the Multipart Request Parser in Django 3.2 before 3.2.18, 4.0 before 4.0.10, and 4.1 before 4.1.7. Passing certain inputs (e.g., an excessive number of parts) to multipart forms could result in too many open files or memory exhaustion, and provided a potential vector for a denial-of-service attack. **CVE ID : CVE-2023-24580**	https://docs.djangoproject.com/en/4.1/releases/security/, https://www.djangoproject.com/weblog/2023/feb/14/security-releases/	A-DJA-DJAN-270223/128
Vendor: dompdf_project					
Product: dompdf					
Affected Version(s): 2.0.1					
Incorrect Authorization	01-Feb-2023	9.8	Dompdf is an HTML to PDF converter. The URI validation on dompdf 2.0.1 can be bypassed on SVG parsing by passing `<image>` tags with uppercase letters. This may lead to arbitrary object unserialize on PHP < 8, through the `phar` URL wrapper. An attacker can exploit the vulnerability to call arbitrary URL with arbitrary protocols, if they can provide a SVG file to dompdf. In PHP	https://github.com/dompdf/dompdf/commit/7558f07f693b2ac3266089f21051e6b78c6a0c85	A-DOM-DOMP-270223/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions before 8.0.0, it leads to arbitrary unserialize, that will lead to the very least to an arbitrary file deletion and even remote code execution, depending on classes that are available. **CVE ID : CVE-2023-23924**		
Affected Version(s): 2.0.2					
Interpretation Conflict	07-Feb-2023	9.8	Dompdf is an HTML to PDF converter written in php. Due to the difference in the attribute parser of Dompdf and php-svg-lib, an attacker can still call arbitrary URLs with arbitrary protocols. Dompdf parses the href attribute of `image` tags and respects `xlink:href` even if `href` is specified. However, php-svg-lib, which is later used to parse the svg file, parses the href attribute. Since `href` is respected if both `xlink:href` and `href` is specified, it's possible to bypass the protection on the Dompdf side by providing an empty `xlink:href` attribute. An attacker can exploit the vulnerability to call arbitrary URLs with arbitrary protocols if they provide an SVG file	https://github.com/dompdf/dompdf/security/advisories/GHSA-56gj-mvh6-rp75, https://github.com/dompdf/dompdf/commit/95009ea98230f9b084b040c34e3869ef3dccc9aa	A-DOM-DOMP-270223/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the Dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, which will lead, at the very least, to arbitrary file deletion and might lead to remote code execution, depending on available classes. This vulnerability has been addressed in commit `95009ea98` which has been included in release version 2.0.3. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-24813**		
Vendor: dst-admin_project					
Product: dst-admin					
Affected Version(s): 1.5.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Feb-2023	7.5	A vulnerability classified as critical was found in dst-admin 1.5.0. Affected by this vulnerability is an unknown functionality of the file /home/cavesConsole. The manipulation of the argument command leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-220033 was	N/A	A-DST-DST--270223/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2023-0646**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Feb-2023	7.5	A vulnerability, which was classified as critical, has been found in dst-admin 1.5.0. Affected by this issue is some unknown functionality of the file /home/kickPlayer. The manipulation of the argument userId leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-220034 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0647**	N/A	A-DST-DST--270223/132
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Feb-2023	7.5	A vulnerability, which was classified as critical, was found in dst-admin 1.5.0. This affects an unknown part of the file /home/masterConsole. The manipulation of the argument command leads to command 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	N/A	A-DST-DST--270223/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-220035. **CVE ID : CVE-2023-0648**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Feb-2023	7.5	A vulnerability has been found in dst-admin 1.5.0 and classified as critical. This vulnerability affects unknown code of the file /home/sendBroadcast. The manipulation of the argument message leads to command injection. 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-220036. **CVE ID : CVE-2023-0649**	N/A	A-DST-DST--270223/134
Vendor: easynas					
Product: easynas					
Affected Version(s): 1.1.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Feb-2023	8.8	A vulnerability classified as critical has been found in EasyNAS 1.1.0. Affected is the function system of the file /backup.pl. The manipulation leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to	N/A	A-EAS-EASY-270223/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade the affected component. VDB-220950 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0830**		
Vendor: Eclipse					
Product: vert.x-web					
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.3.8					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Feb-2023	5.3	Vert.x-Web is a set of building blocks for building web applications in the java programming language. When running vertx web applications that serve files using `StaticHandler` on Windows Operating Systems and Windows File Systems, if the mount point is a wildcard (`*`) then an attacker can exfiltrate any class path resource. When computing the relative path to locate the resource, in case of wildcards, the code: `return "/" + rest;` from `Utils.java` returns the user input (without validation) as the segment to lookup. Even though checks are performed to avoid escaping the sandbox, given that the input was not sanitized `\` are not properly handled and an attacker can build a	https://github.com/vert-x3/vertx-web/commit/9e3a783b1d1a731055e9049078b1b1494ece9c15, https://github.com/vert-x3/vertx-web/security/advisories/GHSA-53jx-vvf9-4x38	A-ECL-VERT-270223/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			path that is valid within the classpath. This issue only affects users deploying in windows environments and upgrading is the advised remediation path. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-24815**		
Vendor: editorconfig					
Product: editorconfig					
Affected Version(s): * Up to (excluding) 0.12.6					
Out-of-bounds Write	01-Feb-2023	7.8	A stack buffer overflow exists in the ec_glob function of editorconfig-core-c before v0.12.6 which allowed an attacker to arbitrarily write to the stack and possibly allows remote code execution. editorconfig-core-c v0.12.6 resolved this vulnerability by bound checking all write operations over the p_pcre buffer. **CVE ID : CVE-2023-0341**	https://github.com/editorconfig/editorconfig-core-c/commit/41281ea82fbf24b060a9f69b9c5369350fb0529e, https://litios.github.io/2023/01/14/CVE-2023-0341.html	A-EDI-EDIT-270223/137
Vendor: elecom					
Product: camera_assistant					
Affected Version(s): 1.00					
Untrusted Search Path	15-Feb-2023	7.8	Untrusted search path vulnerability in ELECOM Camera Assistant 1.00 and QuickFileDealer Ver.1.2.1 and earlier	https://www.elecom.co.jp/news/security/20230214-01/	A-ELE-CAME-270223/138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2023-22368**		
Product: quickfiledealer					
Affected Version(s): * Up to (including) 1.2.1					
Untrusted Search Path	15-Feb-2023	7.8	Untrusted search path vulnerability in ELECOM Camera Assistant 1.00 and QuickFileDealer Ver.1.2.1 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2023-22368**	https://www.elecom.co.jp/news/security/20230214-01/	A-ELE-QUIC-270223/139
Vendor: employee_leaves_management_system_project					
Product: employee_leaves_management_system					
Affected Version(s): 1.0					
Weak Password Requirements	02-Feb-2023	9.1	A vulnerability was found in PHPGurukul Employee Leaves Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file changepassword.php. The manipulation of the argument newpassword/confirm password leads to weak password requirements. The attack can be launched remotely. The exploit	N/A	A-EMP-EMPL-270223/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. The identifier VDB-220021 was assigned to this vulnerability. **CVE ID : CVE-2023-0641**		
Vendor: eta.js					
Product: eta					
Affected Version(s): * Up to (excluding) 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Feb-2023	6.1	Eta is an embedded JS templating engine that works inside Node, Deno, and the browser. XSS attack - anyone using the Express API is impacted. The problem has been resolved. Users should upgrade to version 2.0.0. As a workaround, don't pass user supplied things directly to `res.render`. **CVE ID : CVE-2023-23630**	https://github.com/eta-dev/eta/commit/5651392462ee0ff19d77c8481081a99e5b9138dd	A-ETA-ETA-270223/141
Vendor: exactmetrics					
Product: exactmetrics					
Affected Version(s): * Up to (excluding) 7.12.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The ExactMetrics WordPress plugin before 7.12.1 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform	N/A	A-EXA-EXAC-270223/142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0082**		
Vendor: Expressionengine					
Product: expressionengine					
Affected Version(s): * Up to (excluding) 7.2.6					
N/A	09-Feb-2023	8.8	In ExpressionEngine before 7.2.6, remote code execution can be achieved by an authenticated Control Panel user. **CVE ID : CVE-2023-22953**	https://docs.expressionengine.com/latest/installation/changelog.html	A-EXP-EXPR-270223/143
Vendor: F5					
Product: big-ip_access_policy_manager					
Affected Version(s): 13.1.5					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): 17.0.0					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/145
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Uncontrolled Search Path Element	01-Feb-2023	7.8	In versions beginning with 7.2.2 to before 7.2.3.1, a DLL hijacking vulnerability exists in the BIG-IP Edge Client Windows Installer. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K76964818	A-F5-BIG--270223/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22358**		
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/147
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22340		
NULL Pointer Dereference	01-Feb-2023	7.5	On version 14.1.x before 14.1.5.3, and all versions of 13.1.x, when the BIG-IP APM system is configured with all the following elements, undisclosed requests may cause the Traffic Management Microkernel (TMM) to terminate: * An OAuth Server that references an OAuth Provider * An OAuth profile with the Authorization Endpoint set to '/' * An access profile that references the above OAuth profile and is associated with an HTTPS virtual server Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22341**	https://my.f5.com/manage/s/article/K20717585	A-F5-BIG--270223/149
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note:	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
Uncontrolled Search Path Element	01-Feb-2023	6.5	On versions beginning in 7.1.5 to before 7.2.3.1, a DLL hijacking vulnerability exists in the BIG-IP Edge Client for Windows. User interaction and administrative privileges are required to exploit this vulnerability because the victim user needs to run the executable on the system and the attacker requires administrative privileges for modifying the files in the trusted search path. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22283**	https://my.f5.com/manage/s/article/K07143733	A-F5-BIG--270223/151
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/153
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/154
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/155
NULL Pointer	01-Feb-2023	7.5	On version 14.1.x before 14.1.5.3, and all versions of 13.1.x, when the BIG-IP APM system	https://my.f5.com/mana	A-F5-BIG--270223/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			is configured with all the following elements, undisclosed requests may cause the Traffic Management Microkernel (TMM) to terminate: * An OAuth Server that references an OAuth Provider * An OAuth profile with the Authorization Endpoint set to '/' * An access profile that references the above OAuth profile and is associated with an HTTPS virtual server Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22341**	ge/s/article /K20717585	
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article /K08182564	A-F5-BIG--270223/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22842		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/158
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Uncontrolled Search Path Element	01-Feb-2023	7.8	In versions beginning with 7.2.2 to before 7.2.3.1, a DLL hijacking vulnerability exists in the BIG-IP Edge Client Windows Installer. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22358**	https://my.f5.com/manage/s/article/K76964818	A-F5-BIG--270223/160
Uncontrolled Search Path Element	01-Feb-2023	6.5	On versions beginning in 7.1.5 to before 7.2.3.1, a DLL hijacking vulnerability exists in the BIG-IP Edge Client for Windows. User interaction and administrative privileges are required to exploit this vulnerability because the victim user needs to run the executable on the system and the attacker requires administrative privileges for modifying the files in the trusted search path. Note:	https://my.f5.com/manage/s/article/K07143733	A-F5-BIG--270223/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22283**		
Affected Version(s): From (including) 14.1.4.6 Up to (including) 14.1.5					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/162
Affected Version(s): From (including) 14.1.5 Up to (excluding) 14.1.5.3					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/164
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/165
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.1					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/167
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.8					
Uncontrolled Search Path Element	01-Feb-2023	7.8	In versions beginning with 7.2.2 to before 7.2.3.1, a DLL hijacking vulnerability exists in the BIG-IP Edge Client Windows Installer. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22358**	https://my.f5.com/manage/s/article/K76964818	A-F5-BIG--270223/169
Uncontrolled Search Path Element	01-Feb-2023	6.5	On versions beginning in 7.1.5 to before 7.2.3.1, a DLL hijacking vulnerability exists in the BIG-IP Edge Client for Windows. User interaction and administrative privileges are required to exploit this vulnerability because the victim user needs to run the executable on the system and the attacker requires administrative privileges for modifying the files in the trusted search path. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K07143733	A-F5-BIG--270223/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22283**		
Affected Version(s): From (including) 15.1.4 Up to (excluding) 15.1.8					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/171
Affected Version(s): From (including) 15.1.5.1 Up to (including) 15.1.8					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/173
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/175
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**		
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/177
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/179
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Search Path Element	01-Feb-2023	7.8	In versions beginning with 7.2.2 to before 7.2.3.1, a DLL hijacking vulnerability exists in the BIG-IP Edge Client Windows Installer. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22358**	https://my.f5.com/manage/s/article/K76964818	A-F5-BIG--270223/180
Uncontrolled Search Path Element	01-Feb-2023	6.5	On versions beginning in 7.1.5 to before 7.2.3.1, a DLL hijacking vulnerability exists in the BIG-IP Edge Client for Windows. User interaction and administrative privileges are required to exploit this vulnerability because the victim user needs to run the executable on the system and the attacker requires administrative privileges for modifying the files in the trusted search path. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22283**	https://my.f5.com/manage/s/article/K07143733	A-F5-BIG--270223/181
Affected Version(s): From (including) 16.1.2.2 Up to (excluding) 16.1.3.3					
Missing Release of	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2,	https://my.f5.com/mana	A-F5-BIG--270223/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource after Effective Lifetime			and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**	ge/s/article /K58550078	
Affected Version(s): From (including) 16.1.2.2 Up to (including) 16.1.3					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note:	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.2					
Uncontrolled Search Path Element	01-Feb-2023	7.8	In versions beginning with 7.2.2 to before 7.2.3.1, a DLL hijacking vulnerability exists in the BIG-IP Edge Client Windows Installer. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22358**	https://my.f5.com/manage/s/article/K76964818	A-F5-BIG--270223/184
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**		
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/186
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22340		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/188
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**		
Uncontrolled Search Path Element	01-Feb-2023	6.5	On versions beginning in 7.1.5 to before 7.2.3.1, a DLL hijacking vulnerability exists in the BIG-IP Edge Client for Windows. User interaction and administrative privileges are required to exploit this vulnerability because the victim user needs to run the executable on the system and the attacker requires administrative privileges for modifying the files in the trusted search path. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22283**	https://my.f5.com/manage/s/article/K07143733	A-F5-BIG--270223/190
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/192
Affected Version(s): From (including) 7.2.2 Up to (excluding) 7.2.3.1					
Uncontrolled Search Path Element	01-Feb-2023	7.8	In versions beginning with 7.2.2 to before 7.2.3.1, a DLL hijacking vulnerability exists in	https://my.f5.com/manage/s/article/K76964818	A-F5-BIG--270223/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the BIG-IP Edge Client Windows Installer. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22358**		
Uncontrolled Search Path Element	01-Feb-2023	6.5	On versions beginning in 7.1.5 to before 7.2.3.1, a DLL hijacking vulnerability exists in the BIG-IP Edge Client for Windows. User interaction and administrative privileges are required to exploit this vulnerability because the victim user needs to run the executable on the system and the attacker requires administrative privileges for modifying the files in the trusted search path. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22283**	https://my.f5.com/manage/s/article/K07143733	A-F5-BIG--270223/194
Product: big-ip_advanced_firewall_manager					
Affected Version(s): 13.1.5					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): 17.0.0					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note:	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Use of Uninitialized Resource	01-Feb-2023	7.5	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a BIG-IP AFM NAT policy with a destination NAT rule is configured on a FastL4 virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22281**	https://my.f5.com/manage/s/article/K46048342	A-F5-BIG--270223/197
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/199
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/201
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.3					
Use of Uninitialized Resource	01-Feb-2023	7.5	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a BIG-IP AFM NAT policy with a destination NAT rule is configured on a FastL4 virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22281**	https://my.f5.com/manage/s/article/K46048342	A-F5-BIG--270223/203
Allocation of Resources Without	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3,	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/205
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server,	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/207
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x,	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 14.1.4.6 Up to (including) 14.1.5					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): From (including) 14.1.5 Up to (excluding) 14.1.5.3					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/210
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8					
Use of Uninitialized Resource	01-Feb-2023	7.5	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a BIG-IP AFM NAT policy with a destination NAT rule is configured on a FastL4 virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22281**	https://my.f5.com/manage/s/article/K46048342	A-F5-BIG--270223/212
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server,	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/214
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.1					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/216
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 15.1.5.1 Up to (including) 15.1.8					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22374		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.3					
Use of Uninitialized Resource	01-Feb-2023	7.5	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a BIG-IP AFM NAT policy with a destination NAT rule is configured on a FastL4 virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22281**	https://my.f5.com/manage/s/article/K46048342	A-F5-BIG--270223/219
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/221
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**		
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/223
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/225
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 16.1.2.2 Up to (excluding) 16.1.3.3					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/227
Affected Version(s): From (including) 16.1.2.2 Up to (including) 16.1.3					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.2					
Use of Uninitialized Resource	01-Feb-2023	7.5	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a BIG-IP AFM NAT policy with a destination NAT rule is configured on a FastL4 virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K46048342	A-F5-BIG--270223/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22281**		
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/230
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/232
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**		
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/234
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/236
Product: big-ip_advanced_web_application_firewall					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.0 before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a BIG-IP Advanced WAF or BIG-IP ASM security	https://my.f5.com/manage/s/article/K17542533	A-F5-BIG--270223/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			policy is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23552**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.3					
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.0 before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a BIG-IP Advanced WAF or BIG-IP ASM security policy is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23552**	https://my.f5.com/manage/s/article/K17542533	A-F5-BIG--270223/238
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8					
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.0 before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when	https://my.f5.com/manage/s/article/K17542533	A-F5-BIG--270223/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a BIG-IP Advanced WAF or BIG-IP ASM security policy is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23552**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.3					
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.0 before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a BIG-IP Advanced WAF or BIG-IP ASM security policy is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23552**	https://my.f5.com/manage/s/article/K17542533	A-F5-BIG--270223/240
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.2					
Uncontrolled Resource	01-Feb-2023	7.5	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.0 before 15.1.8, 14.1.x	https://my.f5.com/manage/s/article/K17542533	A-F5-BIG--270223/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			before 14.1.5.3, and all versions of 13.1.x, when a BIG-IP Advanced WAF or BIG-IP ASM security policy is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23552**		
Product: big-ip_analytics					
Affected Version(s): 13.1.5					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): 17.0.0					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/243
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/245
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/247
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/249
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/251
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/253
Affected Version(s): From (including) 14.1.4.6 Up to (including) 14.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/254
Affected Version(s): From (including) 14.1.5 Up to (excluding) 14.1.5.3					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note:	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/256
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.1					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/258
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/260
Affected Version(s): From (including) 15.1.4 Up to (excluding) 15.1.8					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**		
Affected Version(s): From (including) 15.1.5.1 Up to (including) 15.1.8					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22374		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/263
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/265
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22664		
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/267
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/269
Affected Version(s): From (including) 16.1.2.2 Up to (excluding) 16.1.3.3					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**		
Affected Version(s): From (including) 16.1.2.2 Up to (including) 16.1.3					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.2					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/272
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22323		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/274
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22422		
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/276
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/278
Product: big-ip_application_acceleration_manager					
Affected Version(s): 13.1.5					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): 17.0.0					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/281
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22340		
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/283
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/285
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.3					
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
Affected Version(s): From (including) 14.1.5 Up to (excluding) 14.1.5.3					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/287
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/289
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.1					
Allocation of Resources Without	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3,	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/291
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 15.1.4 Up to (excluding) 15.1.8					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23555		
Affected Version(s): From (including) 15.1.5.1 Up to (including) 15.1.8					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/294
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/296
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**		
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/298
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note:	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/300
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 16.1.2.2 Up to (excluding) 16.1.3.3					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/302
Affected Version(s): From (including) 16.1.2.2 Up to (including) 16.1.3					
Use of Externally-	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0,	https://my.f5.com/mana	A-F5-BIG--270223/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	ge/s/article/K000130415	
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.2					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note:	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**		
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/305
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/307
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/309
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Product: big-ip_application_security_manager					
Affected Version(s): 17.0.0					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/311
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/312
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/313
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3,	https://my.f5.com/mana	A-F5-BIG--270223/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	ge/s/article /K08182564	
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.0 before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a BIG-IP Advanced WAF or BIG-IP ASM security policy is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23552**	https://my.f5.com/manage/s/article /K17542533	A-F5-BIG--270223/315
URL Redirection to Untrusted	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all	https://my.f5.com/manage/s/article /K95503300	A-F5-BIG--270223/316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22326		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/318
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/320
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.0 before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a BIG-IP Advanced WAF or BIG-IP ASM security policy is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23552**	https://my.f5.com/manage/s/article/K17542533	A-F5-BIG--270223/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/322
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information.	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 14.1.4.6 Up to (including) 14.1.5					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/324
Affected Version(s): From (including) 14.1.5 Up to (excluding) 14.1.5.3					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/326
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/327
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.0 before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a BIG-IP Advanced WAF or BIG-IP ASM security policy is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23552**	https://my.f5.com/manage/s/article/K17542533	A-F5-BIG--270223/328
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/329
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/331
Affected Version(s): From (including) 15.1.4 Up to (excluding) 15.1.8					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note:	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**		
Affected Version(s): From (including) 15.1.5.1 Up to (including) 15.1.8					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/333
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/335
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**		
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/337
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server,	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.0 before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a BIG-IP Advanced WAF or BIG-IP ASM security policy is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23552**	https://my.f5.com/manage/s/article/K17542533	A-F5-BIG--270223/339
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/341
Affected Version(s): From (including) 16.1.2.2 Up to (excluding) 16.1.3.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/342
Affected Version(s): From (including) 16.1.2.2 Up to (including) 16.1.3					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.2					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/344
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/346
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**		
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/348
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.0 before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a BIG-IP Advanced WAF or BIG-IP ASM security policy is configured on a virtual server, undisclosed requests	https://my.f5.com/manage/s/article/K17542533	A-F5-BIG--270223/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23552**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/350
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): 13.1.0					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22374		
Product: big-ip_ddos_hybrid_defender					
Affected Version(s): 13.1.5					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/353
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/355
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note:	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/357
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/359
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/361
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/363
Affected Version(s): From (including) 14.1.4.6 Up to (including) 14.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/364
Affected Version(s): From (including) 14.1.5 Up to (excluding) 14.1.5.3					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note:	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/366
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.1					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/368
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/370
Affected Version(s): From (including) 15.1.4 Up to (excluding) 15.1.8					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**		
Affected Version(s): From (including) 15.1.5.1 Up to (including) 15.1.8					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22374		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/373
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/375
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22664		
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/377
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/379
Affected Version(s): From (including) 16.1.2.2 Up to (excluding) 16.1.3.3					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**		
Affected Version(s): From (including) 16.1.2.2 Up to (including) 16.1.3					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.2					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/382
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**		
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/384
Product: big-ip_domain_name_system					
Affected Version(s): 17.0.0					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	A-F5-BIG--270223/386
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3,	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/388
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3,	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	A-F5-BIG--270223/390
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3,	https://my.f5.com/mana	A-F5-BIG--270223/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	ge/s/article/K08182564	
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/392
Incorrect Permission Assignmen	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3,	https://my.f5.com/mana	A-F5-BIG--270223/393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
t for Critical Resource			15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	ge/s/article /K83284425	
Affected Version(s): From (including) 14.1.4.6 Up to (including) 14.1.5					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): From (including) 14.1.5 Up to (excluding) 14.1.5.3					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/395
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting	https://my.f5.com/manage/s/article/K37708118	A-F5-BIG--270223/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/397
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8					
NULL Pointer	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8,	https://my.f5.com/mana	A-F5-BIG--270223/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	ge/s/article /K34525368	
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.1					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f 5.com/mana ge/s/article /K56412001	A-F5-BIG-- 270223/399
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of	https://my.f 5.com/mana ge/s/article /K08182564	A-F5-BIG-- 270223/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 15.1.4 Up to (excluding) 15.1.8					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/402
Affected Version(s): From (including) 15.1.5.1 Up to (including) 15.1.8					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/404
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/406
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note:	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	A-F5-BIG--270223/408
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/410
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 16.1.2.2 Up to (excluding) 16.1.3.3					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/412
Affected Version(s): From (including) 16.1.2.2 Up to (including) 16.1.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/413
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.2					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**		
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/415
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/417
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	A-F5-BIG--270223/419
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/421
Product: big-ip_edge					
Affected Version(s): -					
Uncontrolled Search	01-Feb-2023	7.8	In versions beginning with 7.2.2 to before 7.2.3.1, a DLL hijacking	https://my.f5.com/mana	A-F5-BIG--270223/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path Element			vulnerability exists in the BIG-IP Edge Client Windows Installer. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22358**	ge/s/article /K76964818	
Uncontrolled Search Path Element	01-Feb-2023	6.5	On versions beginning in 7.1.5 to before 7.2.3.1, a DLL hijacking vulnerability exists in the BIG-IP Edge Client for Windows. User interaction and administrative privileges are required to exploit this vulnerability because the victim user needs to run the executable on the system and the attacker requires administrative privileges for modifying the files in the trusted search path. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22283**	https://my.f5.com/manage/s/article /K07143733	A-F5-BIG--270223/423
Product: big-ip_fraud_protection_service					
Affected Version(s): 13.1.5					
Use of Externally-Controlled	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on	https://my.f5.com/manage/s/article	A-F5-BIG--270223/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Format String			their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	/K000130415	
Affected Version(s): 17.0.0					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/426
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/428
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/430
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.3					
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
Affected Version(s): From (including) 14.1.5 Up to (excluding) 14.1.5.3					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/432
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
URL Redirection to Untrusted	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/434
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.1					
Allocation of	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2,	https://my.f5.com/mana	A-F5-BIG--270223/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resources Without Limits or Throttling			16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	ge/s/article /K56412001	
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article /K08182564	A-F5-BIG--270223/436
Incorrect Permission Assignment for	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1,	https://my.f5.com/mana	A-F5-BIG--270223/437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	ge/s/article /K83284425	
Affected Version(s): From (including) 15.1.4 Up to (excluding) 15.1.8					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article /K24572686	A-F5-BIG--270223/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**		
Affected Version(s): From (including) 15.1.5.1 Up to (including) 15.1.8					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/439
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/441
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**		
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/443
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/445
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 16.1.2.2 Up to (excluding) 16.1.3.3					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/447
Affected Version(s): From (including) 16.1.2.2 Up to (including) 16.1.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/448
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.2					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**		
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/450
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/452
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/454
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Product: big-ip_link_controller					
Affected Version(s): 13.1.5					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 17.0.0					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/457
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/459
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/461
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/463
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/465
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/467
Affected Version(s): From (including) 14.1.4.6 Up to (including) 14.1.5					
Use of Externally-Controlled	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on	https://my.f5.com/manage/s/article	A-F5-BIG--270223/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Format String			their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	/K000130415	
Affected Version(s): From (including) 14.1.5 Up to (excluding) 14.1.5.3					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/470
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.1					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/472
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/474
Affected Version(s): From (including) 15.1.4 Up to (excluding) 15.1.8					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0,	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**		
Affected Version(s): From (including) 15.1.5.1 Up to (including) 15.1.8					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/477
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/478
Buffer Copy	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2	https://my.f5.com/mana	A-F5-BIG--270223/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	ge/s/article/K43881487	
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/481
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22418		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/483
Affected Version(s): From (including) 16.1.2.2 Up to (excluding) 16.1.3.3					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**		
Affected Version(s): From (including) 16.1.2.2 Up to (including) 16.1.3					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/485
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.2					
Missing Release of	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2,	https://my.f5.com/mana	A-F5-BIG--270223/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource after Effective Lifetime			and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**	ge/s/article/K58550078	
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/488
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/490
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22418		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/492
Product: big-ip_local_traffic_manager					
Affected Version(s): 13.1.5					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): 17.0.0					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22374		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/495
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	A-F5-BIG--270223/497
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22842		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/499
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/501
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note:	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	A-F5-BIG--270223/503
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/505
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 14.1.4.6 Up to (including) 14.1.5					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22374		
Affected Version(s): From (including) 14.1.5 Up to (excluding) 14.1.5.3					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/508
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to	https://my.f5.com/manage/s/article/K37708118	A-F5-BIG--270223/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/510
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.1					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/512
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/514
Affected Version(s): From (including) 15.1.4 Up to (excluding) 15.1.8					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**		
Affected Version(s): From (including) 15.1.5.1 Up to (including) 15.1.8					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22374		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/517
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/519
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22664		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	A-F5-BIG--270223/521
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/523
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 16.1.2.2 Up to (excluding) 16.1.3.3					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/525
Affected Version(s): From (including) 16.1.2.2 Up to (including) 16.1.3					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.2					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**		
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/528
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22340		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/530
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	A-F5-BIG--270223/532
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/534
Product: big-ip_policy_enforcement_manager					
Affected Version(s): 13.1.5					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): 17.0.0					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note:	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/537
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/539
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/541
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/543
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/545
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 14.1.4.6 Up to (including) 14.1.5					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22374		
Affected Version(s): From (including) 14.1.5 Up to (excluding) 14.1.5.3					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/548
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.7					
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/550
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.1					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/552
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 15.1.4 Up to (excluding) 15.1.8					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/554
Affected Version(s): From (including) 15.1.5.1 Up to (including) 15.1.8					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/557
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/559
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/561
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information.	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 16.1.2.2 Up to (excluding) 16.1.3.3					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/563
Affected Version(s): From (including) 16.1.2.2 Up to (including) 16.1.3					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.2					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22302		
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/566
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/568
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22664		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/570
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Product: big-ip_service_proxy					
Affected Version(s): 1.6.0					
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/572
Affected Version(s): From (including) 1.5.0 Up to (excluding) 1.6.0					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**		
Product: big-ip_ssl_orchestrator					
Affected Version(s): 13.1.5					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 17.0.0					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/575
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/577
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/579
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.3					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/581
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**		
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/583
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/585
Affected Version(s): From (including) 14.1.4.6 Up to (including) 14.1.5					
Use of Externally-Controlled	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on	https://my.f5.com/manage/s/article	A-F5-BIG--270223/586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Format String			their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	/K000130415	
Affected Version(s): From (including) 14.1.5 Up to (excluding) 14.1.5.3					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/588
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.1					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**		
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/590
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22418**		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/592
Affected Version(s): From (including) 15.1.4 Up to (excluding) 15.1.8					
Improper Initialization	01-Feb-2023	7.5	On BIG-IP Virtual Edition versions 15.1x beginning in 15.1.4 to before 15.1.8 and 14.1.x beginning in 14.1.5 to before 14.1.5.3, and BIG-IP SPK beginning in 1.5.0 to before 1.6.0, when FastL4 profile is	https://my.f5.com/manage/s/article/K24572686	A-F5-BIG--270223/593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-23555**		
Affected Version(s): From (including) 15.1.5.1 Up to (including) 15.1.8					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/594
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/595
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/596
Buffer Copy without Checking	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP	https://my.f5.com/mana	A-F5-BIG--270223/597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	ge/s/article/K43881487	
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22842**	https://my.f5.com/manage/s/article/K08182564	A-F5-BIG--270223/599
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22418		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/601
Affected Version(s): From (including) 16.1.2.2 Up to (excluding) 16.1.3.3					
Missing Release of Resource after Effective Lifetime	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2, and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can	https://my.f5.com/manage/s/article/K58550078	A-F5-BIG--270223/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**		
Affected Version(s): From (including) 16.1.2.2 Up to (including) 16.1.3					
Use of Externally-Controlled Format String	01-Feb-2023	9.9	In BIG-IP starting in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5 on their respective branches, a format string vulnerability exists in iControl SOAP that allows an authenticated attacker to crash the iControl SOAP CGI process or, potentially execute arbitrary code. In appliance mode BIG-IP, a successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22374**	https://my.f5.com/manage/s/article/K000130415	A-F5-BIG--270223/603
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.0.2					
Missing Release of	01-Feb-2023	7.5	In BIG-IP versions 17.0.x before 17.0.0.2,	https://my.f5.com/mana	A-F5-BIG--270223/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource after Effective Lifetime			and 16.1.x beginning in 16.1.2.2 to before 16.1.3.3, when an HTTP profile is configured on a virtual server and conditions beyond the attacker's control exist on the target pool member, undisclosed requests sent to the BIG-IP system can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22302**	ge/s/article/K58550078	
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OCSP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22323**	https://my.f5.com/manage/s/article/K56412001	A-F5-BIG--270223/605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 16.1.x before 16.1.3.3, 15.1.x before 15.1.8, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when a SIP profile is configured on a Message Routing type virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22340**	https://my.f5.com/manage/s/article/K34525368	A-F5-BIG--270223/606
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, when a HTTP profile with the non-default Enforcement options of Enforce HTTP Compliance and Unknown Methods: Reject are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22422**	https://my.f5.com/manage/s/article/K43881487	A-F5-BIG--270223/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2 and 16.1.x before 16.1.3.3, and BIG-IP SPK starting in version 1.6.0, when a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22664**	https://my.f5.com/manage/s/article/K56676554	A-F5-BIG--270223/608
URL Redirection to Untrusted Site ('Open Redirect')	01-Feb-2023	6.1	On versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.7, 14.1.x before 14.1.5.3, and all versions of 13.1.x, an open redirect vulnerability exists on virtual servers enabled with a BIG-IP APM access policy. This vulnerability allows an unauthenticated malicious attacker to build an open redirect URI. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K95503300	A-F5-BIG--270223/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22418		
Incorrect Permission Assignment for Critical Resource	01-Feb-2023	4.9	In BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, and all versions of BIG-IQ 8.x and 7.1.x, incorrect permission assignment vulnerabilities exist in the iControl REST and TMOS shell (tmsh) dig command which may allow an authenticated attacker with resource administrator or administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22326**	https://my.f5.com/manage/s/article/K83284425	A-F5-BIG--270223/610
Vendor: farsight					
Product: provide_server					
Affected Version(s): 14.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Feb-2023	6.1	Cross Site Scripting (XSS) vulnerability in Provide server 14.4 allows attackers to execute arbitrary code through the server-log via username field from the login form.	N/A	A-FAR-PROV-270223/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23286		
Vendor: fastcms_project					
Product: fastcms					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	02-Feb-2023	9.8	A vulnerability was found in FastCMS 0.1.0. It has been classified as critical. Affected is an unknown function of the component Template Management. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-220038 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0651**	N/A	A-FAS-FAST-270223/612
Vendor: fastify					
Product: fastify-multipart					
Affected Version(s): * Up to (excluding) 6.0.1					
Allocation of Resources Without Limits or Throttling	14-Feb-2023	7.5	@fastify/multipart is a Fastify plugin to parse the multipart content-type. Prior to versions 7.4.1 and 6.0.1, @fastify/multipart may experience denial of service due to a number of situations in which an unlimited number of parts are accepted. This includes the multipart body parser accepting an unlimited number of	https://github.com/fastify/fastify-multipart/commit/85be81bedf5b29cfd9fe3efc30fb5a17173c1297	A-FAS-FAST-270223/613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file parts, the multipart body parser accepting an unlimited number of field parts, and the multipart body parser accepting an unlimited number of empty parts as field parts. This is fixed in v7.4.1 (for Fastify v4.x) and v6.0.1 (for Fastify v3.x). There are no known workarounds. **CVE ID : CVE-2023-25576**		
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.4.1					
Allocation of Resources Without Limits or Throttling	14-Feb-2023	7.5	@fastify/multipart is a Fastify plugin to parse the multipart content-type. Prior to versions 7.4.1 and 6.0.1, @fastify/multipart may experience denial of service due to a number of situations in which an unlimited number of parts are accepted. This includes the multipart body parser accepting an unlimited number of file parts, the multipart body parser accepting an unlimited number of field parts, and the multipart body parser accepting an unlimited number of empty parts as field parts. This is fixed in v7.4.1 (for Fastify v4.x) and v6.0.1 (for Fastify v3.x). There are no known workarounds.	https://github.com/fastify/fastify-multipart/commit/85be81bedf5b29cfd9fe3efc30fb5a17173c1297	A-FAS-FAST-270223/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25576		
Vendor: flexible_captcha_project					
Product: flexible_captcha					
Affected Version(s): * Up to (including) 4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The Flexible Captcha WordPress plugin through 4.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0147**	N/A	A-FLE-FLEX-270223/615
Vendor: Foliovision					
Product: fv_flowplayer_video_player					
Affected Version(s): * Up to (including) 7.5.30.7212					
Cross-Site Request Forgery (CSRF)	14-Feb-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in FolioVision FV Flowplayer Video Player plugin <= 7.5.30.7212 versions. **CVE ID : CVE-2023-25066**	N/A	A-FOL-FV_F-270223/616
Vendor: forget_heart_message_box_project					
Product: forget_heart_message_box					
Affected Version(s): 1.1					
Improper Neutralization of	01-Feb-2023	9.8	Forget Heart Message Box v1.1 was discovered to contain a	N/A	A-FOR-FORG-270223/617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			SQL injection vulnerability via the name parameter at /admin/loginpost.php. **CVE ID : CVE-2023-24241**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Feb-2023	8.8	Forget Heart Message Box v1.1 was discovered to contain a SQL injection vulnerability via the name parameter at /cha.php. **CVE ID : CVE-2023-24956**	N/A	A-FOR-FORG-270223/618
Vendor: formwork_project					
Product: formwork					
Affected Version(s): 1.12.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Feb-2023	4.8	A stored cross-site scripting (XSS) vulnerability in the component /formwork/panel/dashboard of Formwork v1.12.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Page title parameter. **CVE ID : CVE-2023-24230**	N/A	A-FOR-FORM-270223/619
Vendor: fortra					
Product: goanywhere_managed_file_transfer					
Affected Version(s): * Up to (excluding) 7.1.2					
Deserialization of	06-Feb-2023	7.2	Fortra (formerly, HelpSystems) GoAnywhere MFT	https://github.com/rapid7/metasplo	A-FOR-GOAN-270223/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			suffers from a pre-authentication command injection vulnerability in the License Response Servlet due to deserializing an arbitrary attacker-controlled object. This issue was patched in version 7.1.2. **CVE ID : CVE-2023-0669**	it-framework/pull/17607	
Vendor: Froxlor					
Product: froxlor					
Affected Version(s): * Up to (excluding) 2.0.10					
Improper Control of Generation of Code ('Code Injection')	04-Feb-2023	8.8	Code Injection in GitHub repository froxlor/froxlor prior to 2.0.10. **CVE ID : CVE-2023-0671**	https://huntr.dev/bounties/c2a84917-7ac0-4169-81c1-b61e617023de, https://github.com/froxlor/froxlor/commit/0034681412057fef2dfe9cce9f8a6e3321f52edc	A-FRO-FROX-270223/621
Vendor: ftdms_project					
Product: ftdms					
Affected Version(s): 3.1.6					
Unrestricted Upload of File with Dangerous Type	01-Feb-2023	7.2	An arbitrary file upload vulnerability in Ftdms v3.1.6 allows attackers to execute arbitrary code via uploading a crafted JPG file.	N/A	A-FTD-FTDM-270223/622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23135		
Vendor: Fujitsu					
Product: tsclinical_define.xml_generator					
Affected Version(s): From (including) 1.0.0 Up to (including) 1.4.0					
Improper Restriction of XML External Entity Reference	15-Feb-2023	7.4	Improper restriction of XML external entity reference (XXE) vulnerability exists in tsClinical Define.xml Generator all versions (v1.0.0 to v1.4.0) and tsClinical Metadata Desktop Tools Version 1.0.3 to Version 1.1.0. If this vulnerability is exploited, an attacker may obtain an arbitrary file which meets a certain condition by reading a specially crafted XML file. **CVE ID : CVE-2023-22377**	N/A	A-FUJ-TSCL-270223/623
Product: tsclinical_metadata_desktop_tools					
Affected Version(s): From (including) 1.0.3 Up to (excluding) 1.1.1					
Improper Restriction of XML External Entity Reference	15-Feb-2023	7.4	Improper restriction of XML external entity reference (XXE) vulnerability exists in tsClinical Define.xml Generator all versions (v1.0.0 to v1.4.0) and tsClinical Metadata Desktop Tools Version 1.0.3 to Version 1.1.0. If this vulnerability is exploited, an attacker may obtain an arbitrary file which meets a certain condition by	N/A	A-FUJ-TSCL-270223/624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reading a specially crafted XML file. **CVE ID : CVE-2023-22377**		
Vendor: gamipress					
Product: gamipress					
Affected Version(s): * Up to (excluding) 1.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The GamiPress WordPress plugin before 1.0.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0154**	N/A	A-GAM-GAMI-270223/625
Vendor: getlasso					
Product: simple_urls					
Affected Version(s): * Up to (excluding) 115					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Feb-2023	8.8	The Simple URLs WordPress plugin before 115 does not escape some parameters before using them in various SQL statements used by AJAX actions available by any authenticated users, leading to a SQL injection exploitable by low privilege users such as subscriber.	N/A	A-GET-SIMP-270223/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0098		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	6.1	The Simple URLs WordPress plugin before 115 does not sanitise and escape some parameters before outputting them back in some pages, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin. **CVE ID : CVE-2023-0099**	N/A	A-GET-SIMP-270223/627
Vendor: getwpfunnels					
Product: drag_\&_drop_sales_funnel_builder					
Affected Version(s): * Up to (excluding) 2.6.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The Drag & Drop Sales Funnel Builder for WordPress plugin before 2.6.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0173**	N/A	A-GET-DRAG-270223/628
Vendor: Git-scm					
Product: git					
Affected Version(s): * Up to (excluding) 2.30.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Feb-2023	7.5	Git, a revision control system, is vulnerable to path traversal prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8. By feeding a crafted input to `git apply`, a path outside the working tree can be overwritten as the user who is running `git apply`. A fix has been prepared and will appear in v2.39.2, v2.38.4, v2.37.6, v2.36.5, v2.35.7, v2.34.7, v2.33.7, v2.32.6, v2.31.7, and v2.30.8. As a workaround, use `git apply --stat` to inspect a patch before applying; avoid applying one that creates a symbolic link and then creates a file beyond the symbolic link. **CVE ID : CVE-2023-23946**	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-r87m-v37r-cwfh	A-GIT-GIT-270223/629
Improper Link Resolution Before File Access ('Link Following')	14-Feb-2023	5.5	Git is a revision control system. Using a specially-crafted repository, Git prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8 can be tricked into using its local clone optimization even when using a non-local transport. Though Git will abort local	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-gw92-x3fm-3g3q,	A-GIT-GIT-270223/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clones whose source `$GIT_DIR/objects` directory contains symbolic links, the `objects` directory itself may still be a symbolic link. These two may be combined to include arbitrary files based on known paths on the victim's filesystem within the malicious repository's working copy, allowing for data exfiltration in a similar manner as CVE-2022-39253. A fix has been prepared and will appear in v2.39.2 v2.38.4 v2.37.6 v2.36.5 v2.35.7 v2.34.7 v2.33.7 v2.32.6, v2.31.7 and v2.30.8. If upgrading is impractical, two short-term workarounds are available. Avoid cloning repositories from untrusted sources with `--recurse-submodules`. Instead, consider cloning repositories without recursively cloning their submodules, and instead run `git submodule update` at each layer. Before doing so, inspect each new `.gitmodules` file to ensure that it does not contain suspicious module URLs.	https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22490		
Affected Version(s): * Up to (excluding) 2.39.2					
Untrusted Search Path	14-Feb-2023	7.3	Git for Windows is the Windows port of the revision control system Git. Prior to Git for Windows version 2.39.2, by carefully crafting DLL and putting into a subdirectory of a specific name living next to the Git for Windows installer, Windows can be tricked into side-loading said DLL. This potentially allows users with local write access to place malicious payloads in a location where automated upgrades might run the Git for Windows installer with elevation. Version 2.39.2 contains a patch for this issue. Some workarounds are available. Never leave untrusted files in the Downloads folder or its sub-folders before executing the Git for Windows installer, or move the installer into a different directory before executing it. **CVE ID : CVE-2023-22743**	https://github.com/git-for-windows/git/security/advisories/GHSA-gf48-x3vr-j5c3, https://github.com/git-for-windows/git/security/advisories/GHSA-p2x9-prp4-8gvq	A-GIT-GIT-270223/631
Affected Version(s): From (including) 2.31.0 Up to (excluding) 2.31.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Feb-2023	7.5	Git, a revision control system, is vulnerable to path traversal prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8. By feeding a crafted input to `git apply`, a path outside the working tree can be overwritten as the user who is running `git apply`. A fix has been prepared and will appear in v2.39.2, v2.38.4, v2.37.6, v2.36.5, v2.35.7, v2.34.7, v2.33.7, v2.32.6, v2.31.7, and v2.30.8. As a workaround, use `git apply --stat` to inspect a patch before applying; avoid applying one that creates a symbolic link and then creates a file beyond the symbolic link. **CVE ID : CVE-2023-23946**	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-r87m-v37r-cwfh	A-GIT-GIT-270223/632
Improper Link Resolution Before File Access ('Link Following')	14-Feb-2023	5.5	Git is a revision control system. Using a specially-crafted repository, Git prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8 can be tricked into using its local clone optimization even when using a non-local transport. Though Git will abort local	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-gw92-x3fm-3g3q,	A-GIT-GIT-270223/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clones whose source `$GIT_DIR/objects` directory contains symbolic links, the `objects` directory itself may still be a symbolic link. These two may be combined to include arbitrary files based on known paths on the victim's filesystem within the malicious repository's working copy, allowing for data exfiltration in a similar manner as CVE-2022-39253. A fix has been prepared and will appear in v2.39.2 v2.38.4 v2.37.6 v2.36.5 v2.35.7 v2.34.7 v2.33.7 v2.32.6, v2.31.7 and v2.30.8. If upgrading is impractical, two short-term workarounds are available. Avoid cloning repositories from untrusted sources with `--recurse-submodules`. Instead, consider cloning repositories without recursively cloning their submodules, and instead run `git submodule update` at each layer. Before doing so, inspect each new `.gitmodules` file to ensure that it does not contain suspicious module URLs.	https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22490		
Affected Version(s): From (including) 2.32.0 Up to (excluding) 2.32.6					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Feb-2023	7.5	Git, a revision control system, is vulnerable to path traversal prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8. By feeding a crafted input to `git apply`, a path outside the working tree can be overwritten as the user who is running `git apply`. A fix has been prepared and will appear in v2.39.2, v2.38.4, v2.37.6, v2.36.5, v2.35.7, v2.34.7, v2.33.7, v2.32.6, v2.31.7, and v2.30.8. As a workaround, use `git apply --stat` to inspect a patch before applying; avoid applying one that creates a symbolic link and then creates a file beyond the symbolic link. **CVE ID : CVE-2023-23946**	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-r87m-v37r-cwfh	A-GIT-GIT-270223/634
Improper Link Resolution Before File Access ('Link Following')	14-Feb-2023	5.5	Git is a revision control system. Using a specially-crafted repository, Git prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8 can be tricked into using its local clone optimization	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/	A-GIT-GIT-270223/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			even when using a non-local transport. Though Git will abort local clones whose source `$GIT_DIR/objects` directory contains symbolic links, the `objects` directory itself may still be a symbolic link. These two may be combined to include arbitrary files based on known paths on the victim's filesystem within the malicious repository's working copy, allowing for data exfiltration in a similar manner as CVE-2022-39253. A fix has been prepared and will appear in v2.39.2 v2.38.4 v2.37.6 v2.36.5 v2.35.7 v2.34.7 v2.33.7 v2.32.6, v2.31.7 and v2.30.8. If upgrading is impractical, two short-term workarounds are available. Avoid cloning repositories from untrusted sources with `--recurse-submodules`. Instead, consider cloning repositories without recursively cloning their submodules, and instead run `git submodule update` at each layer. Before doing so, inspect each new `.gitmodules` file to ensure that it does not	advisories/GHSA-gw92-x3fm-3g3q, https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain suspicious module URLs. **CVE ID : CVE-2023-22490**		
Affected Version(s): From (including) 2.33.0 Up to (excluding) 2.33.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Feb-2023	7.5	Git, a revision control system, is vulnerable to path traversal prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8. By feeding a crafted input to `git apply`, a path outside the working tree can be overwritten as the user who is running `git apply`. A fix has been prepared and will appear in v2.39.2, v2.38.4, v2.37.6, v2.36.5, v2.35.7, v2.34.7, v2.33.7, v2.32.6, v2.31.7, and v2.30.8. As a workaround, use `git apply --stat` to inspect a patch before applying; avoid applying one that creates a symbolic link and then creates a file beyond the symbolic link. **CVE ID : CVE-2023-23946**	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-r87m-v37r-cwfh	A-GIT-GIT-270223/636
Improper Link Resolution Before File Access ('Link Following')	14-Feb-2023	5.5	Git is a revision control system. Using a specially-crafted repository, Git prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6,	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd,	A-GIT-GIT-270223/637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.31.7, and 2.30.8 can be tricked into using its local clone optimization even when using a non-local transport. Though Git will abort local clones whose source `$GIT_DIR/objects` directory contains symbolic links, the `objects` directory itself may still be a symbolic link. These two may be combined to include arbitrary files based on known paths on the victim's filesystem within the malicious repository's working copy, allowing for data exfiltration in a similar manner as CVE-2022-39253. A fix has been prepared and will appear in v2.39.2 v2.38.4 v2.37.6 v2.36.5 v2.35.7 v2.34.7 v2.33.7 v2.32.6, v2.31.7 and v2.30.8. If upgrading is impractical, two short-term workarounds are available. Avoid cloning repositories from untrusted sources with `--recurse-submodules`. Instead, consider cloning repositories without recursively cloning their submodules, and instead run `git submodule update` at each layer. Before doing so, inspect each new	https://github.com/git/git/security/advisories/GHSA-gw92-x3fm-3g3q, https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`.gitmodules` file to ensure that it does not contain suspicious module URLs. **CVE ID : CVE-2023-22490**		
Affected Version(s): From (including) 2.34.0 Up to (excluding) 2.34.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Feb-2023	7.5	Git, a revision control system, is vulnerable to path traversal prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8. By feeding a crafted input to `git apply`, a path outside the working tree can be overwritten as the user who is running `git apply`. A fix has been prepared and will appear in v2.39.2, v2.38.4, v2.37.6, v2.36.5, v2.35.7, v2.34.7, v2.33.7, v2.32.6, v2.31.7, and v2.30.8. As a workaround, use `git apply --stat` to inspect a patch before applying; avoid applying one that creates a symbolic link and then creates a file beyond the symbolic link. **CVE ID : CVE-2023-23946**	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-r87m-v37r-cwfh	A-GIT-GIT-270223/638
Improper Link Resolution Before File Access	14-Feb-2023	5.5	Git is a revision control system. Using a specially-crafted repository, Git prior to versions 2.39.2, 2.38.4,	https://github.com/git/git/commit/c867e4fa180bec4750e9b	A-GIT-GIT-270223/639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Link Following')			2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8 can be tricked into using its local clone optimization even when using a non-local transport. Though Git will abort local clones whose source `$GIT_DIR/objects` directory contains symbolic links, the `objects` directory itself may still be a symbolic link. These two may be combined to include arbitrary files based on known paths on the victim's filesystem within the malicious repository's working copy, allowing for data exfiltration in a similar manner as CVE-2022-39253. A fix has been prepared and will appear in v2.39.2 v2.38.4 v2.37.6 v2.36.5 v2.35.7 v2.34.7 v2.33.7 v2.32.6, v2.31.7 and v2.30.8. If upgrading is impractical, two short-term workarounds are available. Avoid cloning repositories from untrusted sources with `--recurse-submodules`. Instead, consider cloning repositories without recursively cloning their submodules, and instead run `git submodule update` at	54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-gw92-x3fm-3g3q, https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			each layer. Before doing so, inspect each new `.gitmodules` file to ensure that it does not contain suspicious module URLs. **CVE ID : CVE-2023-22490**		
Affected Version(s): From (including) 2.35.0 Up to (excluding) 2.35.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Feb-2023	7.5	Git, a revision control system, is vulnerable to path traversal prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8. By feeding a crafted input to `git apply`, a path outside the working tree can be overwritten as the user who is running `git apply`. A fix has been prepared and will appear in v2.39.2, v2.38.4, v2.37.6, v2.36.5, v2.35.7, v2.34.7, v2.33.7, v2.32.6, v2.31.7, and v2.30.8. As a workaround, use `git apply --stat` to inspect a patch before applying; avoid applying one that creates a symbolic link and then creates a file beyond the symbolic link. **CVE ID : CVE-2023-23946**	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-r87m-v37r-cwfh	A-GIT-GIT-270223/640
Improper Link Resolution	14-Feb-2023	5.5	Git is a revision control system. Using a specially-crafted	https://github.com/git/git/commit/	A-GIT-GIT-270223/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Before File Access ('Link Following')			repository, Git prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8 can be tricked into using its local clone optimization even when using a non-local transport. Though Git will abort local clones whose source `$GIT_DIR/objects` directory contains symbolic links, the `objects` directory itself may still be a symbolic link. These two may be combined to include arbitrary files based on known paths on the victim's filesystem within the malicious repository's working copy, allowing for data exfiltration in a similar manner as CVE-2022-39253. A fix has been prepared and will appear in v2.39.2 v2.38.4 v2.37.6 v2.36.5 v2.35.7 v2.34.7 v2.33.7 v2.32.6, v2.31.7 and v2.30.8. If upgrading is impractical, two short-term workarounds are available. Avoid cloning repositories from untrusted sources with `--recurse-submodules`. Instead, consider cloning repositories without recursively cloning their submodules, and	c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-gw92-x3fm-3g3q, https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			instead run `git submodule update` at each layer. Before doing so, inspect each new `.gitmodules` file to ensure that it does not contain suspicious module URLs. **CVE ID : CVE-2023-22490**		
Affected Version(s): From (including) 2.36.0 Up to (excluding) 2.36.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Feb-2023	7.5	Git, a revision control system, is vulnerable to path traversal prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8. By feeding a crafted input to `git apply`, a path outside the working tree can be overwritten as the user who is running `git apply`. A fix has been prepared and will appear in v2.39.2, v2.38.4, v2.37.6, v2.36.5, v2.35.7, v2.34.7, v2.33.7, v2.32.6, v2.31.7, and v2.30.8. As a workaround, use `git apply --stat` to inspect a patch before applying; avoid applying one that creates a symbolic link and then creates a file beyond the symbolic link. **CVE ID : CVE-2023-23946**	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-r87m-v37r-cwfh	A-GIT-GIT-270223/642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Link Resolution Before File Access ('Link Following')	14-Feb-2023	5.5	Git is a revision control system. Using a specially-crafted repository, Git prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8 can be tricked into using its local clone optimization even when using a non-local transport. Though Git will abort local clones whose source `$GIT_DIR/objects` directory contains symbolic links, the `objects` directory itself may still be a symbolic link. These two may be combined to include arbitrary files based on known paths on the victim's filesystem within the malicious repository's working copy, allowing for data exfiltration in a similar manner as CVE-2022-39253. A fix has been prepared and will appear in v2.39.2 v2.38.4 v2.37.6 v2.36.5 v2.35.7 v2.34.7 v2.33.7 v2.32.6, v2.31.7 and v2.30.8. If upgrading is impractical, two short-term workarounds are available. Avoid cloning repositories from untrusted sources with `--recurse-submodules`. Instead, consider cloning repositories	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-gw92-x3fm-3g3q, https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	A-GIT-GIT-270223/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without recursively cloning their submodules, and instead run `git submodule update` at each layer. Before doing so, inspect each new `.gitmodules` file to ensure that it does not contain suspicious module URLs. **CVE ID : CVE-2023-22490**		
Affected Version(s): From (including) 2.37.0 Up to (excluding) 2.37.6					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Feb-2023	7.5	Git, a revision control system, is vulnerable to path traversal prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8. By feeding a crafted input to `git apply`, a path outside the working tree can be overwritten as the user who is running `git apply`. A fix has been prepared and will appear in v2.39.2, v2.38.4, v2.37.6, v2.36.5, v2.35.7, v2.34.7, v2.33.7, v2.32.6, v2.31.7, and v2.30.8. As a workaround, use `git apply --stat` to inspect a patch before applying; avoid applying one that creates a symbolic link and then creates a file beyond the symbolic link.	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-r87m-v37r-cwfh	A-GIT-GIT-270223/644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23946		
Improper Link Resolution Before File Access ('Link Following')	14-Feb-2023	5.5	Git is a revision control system. Using a specially-crafted repository, Git prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8 can be tricked into using its local clone optimization even when using a non-local transport. Though Git will abort local clones whose source `$GIT_DIR/objects` directory contains symbolic links, the `objects` directory itself may still be a symbolic link. These two may be combined to include arbitrary files based on known paths on the victim's filesystem within the malicious repository's working copy, allowing for data exfiltration in a similar manner as CVE-2022-39253. A fix has been prepared and will appear in v2.39.2 v2.38.4 v2.37.6 v2.36.5 v2.35.7 v2.34.7 v2.33.7 v2.32.6, v2.31.7 and v2.30.8. If upgrading is impractical, two short-term workarounds are available. Avoid cloning repositories from untrusted sources with `--recurse-submodules`.	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-gw92-x3fm-3g3q, https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	A-GIT-GIT-270223/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Instead, consider cloning repositories without recursively cloning their submodules, and instead run `git submodule update` at each layer. Before doing so, inspect each new `.gitmodules` file to ensure that it does not contain suspicious module URLs. **CVE ID : CVE-2023-22490**		
Affected Version(s): From (including) 2.38.0 Up to (excluding) 2.38.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Feb-2023	7.5	Git, a revision control system, is vulnerable to path traversal prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8. By feeding a crafted input to `git apply`, a path outside the working tree can be overwritten as the user who is running `git apply`. A fix has been prepared and will appear in v2.39.2, v2.38.4, v2.37.6, v2.36.5, v2.35.7, v2.34.7, v2.33.7, v2.32.6, v2.31.7, and v2.30.8. As a workaround, use `git apply --stat` to inspect a patch before applying; avoid applying one that creates a symbolic link and then creates a file	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-r87m-v37r-cwfh	A-GIT-GIT-270223/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beyond the symbolic link. **CVE ID : CVE-2023-23946**		
Improper Link Resolution Before File Access ('Link Following')	14-Feb-2023	5.5	Git is a revision control system. Using a specially-crafted repository, Git prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8 can be tricked into using its local clone optimization even when using a non-local transport. Though Git will abort local clones whose source `$GIT_DIR/objects` directory contains symbolic links, the `objects` directory itself may still be a symbolic link. These two may be combined to include arbitrary files based on known paths on the victim's filesystem within the malicious repository's working copy, allowing for data exfiltration in a similar manner as CVE-2022-39253. A fix has been prepared and will appear in v2.39.2 v2.38.4 v2.37.6 v2.36.5 v2.35.7 v2.34.7 v2.33.7 v2.32.6, v2.31.7 and v2.30.8. If upgrading is impractical, two short-term workarounds are available. Avoid cloning	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-gw92-x3fm-3g3q, https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	A-GIT-GIT-270223/647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			repositories from untrusted sources with `--recurse-submodules`. Instead, consider cloning repositories without recursively cloning their submodules, and instead run `git submodule update` at each layer. Before doing so, inspect each new `.gitmodules` file to ensure that it does not contain suspicious module URLs. **CVE ID : CVE-2023-22490**		
Affected Version(s): From (including) 2.39.0 Up to (excluding) 2.39.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Feb-2023	7.5	Git, a revision control system, is vulnerable to path traversal prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8. By feeding a crafted input to `git apply`, a path outside the working tree can be overwritten as the user who is running `git apply`. A fix has been prepared and will appear in v2.39.2, v2.38.4, v2.37.6, v2.36.5, v2.35.7, v2.34.7, v2.33.7, v2.32.6, v2.31.7, and v2.30.8. As a workaround, use `git apply --stat` to inspect a patch before applying; avoid applying one that	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-r87m-v37r-cwfh	A-GIT-GIT-270223/648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			creates a symbolic link and then creates a file beyond the symbolic link. **CVE ID : CVE-2023-23946**		
Improper Link Resolution Before File Access ('Link Following')	14-Feb-2023	5.5	Git is a revision control system. Using a specially-crafted repository, Git prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8 can be tricked into using its local clone optimization even when using a non-local transport. Though Git will abort local clones whose source `$GIT_DIR/objects` directory contains symbolic links, the `objects` directory itself may still be a symbolic link. These two may be combined to include arbitrary files based on known paths on the victim's filesystem within the malicious repository's working copy, allowing for data exfiltration in a similar manner as CVE-2022-39253. A fix has been prepared and will appear in v2.39.2 v2.38.4 v2.37.6 v2.36.5 v2.35.7 v2.34.7 v2.33.7 v2.32.6, v2.31.7 and v2.30.8. If upgrading is impractical, two short-	https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd, https://github.com/git/git/security/advisories/GHSA-gw92-x3fm-3g3q, https://github.com/git/git/security/advisories/GHSA-3wp6-j8xr-qw85	A-GIT-GIT-270223/649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			term workarounds are available. Avoid cloning repositories from untrusted sources with `--recurse-submodules`. Instead, consider cloning repositories without recursively cloning their submodules, and instead run `git submodule update` at each layer. Before doing so, inspect each new `.gitmodules` file to ensure that it does not contain suspicious module URLs. **CVE ID : CVE-2023-22490**		
Vendor: git_for_windows_project					
Product: git_for_windows					
Affected Version(s): * Up to (excluding) 2.39.2					
Untrusted Search Path	14-Feb-2023	7.8	Git for Windows is the Windows port of the revision control system Git. Prior to Git for Windows version 2.39.2, when `gitk` is run on Windows, it potentially runs executables from the current directory inadvertently, which can be exploited with some social engineering to trick users into running untrusted code. A patch is available in version 2.39.2. As a workaround, avoid using `gitk` (or Git GUI's	https://github.com/git-for-windows/git/security/advisories/GHSA-wxwv-49qw-35pm, https://github.com/git-for-windows/git/commit/49a8ec9dac3cec6602f05fed1b3f80a549c8c05c	A-GIT-GIT_-270223/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"Visualize History" functionality) in clones of untrusted repositories. **CVE ID : CVE-2023-23618**		
Affected Version(s): * Up to (excluding) 2.35.2					
Untrusted Search Path	14-Feb-2023	7.3	Git for Windows is the Windows port of the revision control system Git. Prior to Git for Windows version 2.39.2, by carefully crafting DLL and putting into a subdirectory of a specific name living next to the Git for Windows installer, Windows can be tricked into side-loading said DLL. This potentially allows users with local write access to place malicious payloads in a location where automated upgrades might run the Git for Windows installer with elevation. Version 2.39.2 contains a patch for this issue. Some workarounds are available. Never leave untrusted files in the Downloads folder or its sub-folders before executing the Git for Windows installer, or move the installer into a different directory before executing it.	https://github.com/git-for-windows/git/security/advisories/GHSA-gf48-x3vr-j5c3, https://github.com/git-for-windows/git/security/advisories/GHSA-p2x9-prp4-8gvq	A-GIT-GIT_-270223/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22743		
Vendor: GNU					
Product: glibc					
Affected Version(s): 2.37					
Out-of-bounds Write	03-Feb-2023	9.8	sprintf in the GNU C Library (glibc) 2.37 has a buffer overflow (out-of-bounds write) in some situations with a correct buffer size. This is unrelated to CWE-676. It may write beyond the bounds of the destination buffer when attempting to write a padded, thousands-separated string representation of a number, if the buffer is allocated the exact size required to represent that number as a string. For example, 1,234,567 (with padding to 13) overflows by two bytes. **CVE ID : CVE-2023-25139**	N/A	A-GNU-GLIB-270223/652
Affected Version(s): 2.38					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Feb-2023	9.8	** DISPUTED ** A vulnerability was found in GNU C Library 2.38. It has been declared as critical. This vulnerability affects the function __monstartup of the file gmon.c of the component Call Graph Monitor. The manipulation leads to buffer overflow. It is	https://sourceware.org/bugzilla/show_bug.cgi?id=29444, https://patchwork.sourceware.org/project/glibc/patch/20230204114138.5436-1-	A-GNU-GLIB-270223/653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recommended to apply a patch to fix this issue. VDB-220246 is the identifier assigned to this vulnerability. NOTE: The real existence of this vulnerability is still doubted at the moment. The inputs that induce this vulnerability are basically addresses of the running application that is built with gmon enabled. It's basically trusted input or input that needs an actual security flaw to be compromised or controlled. **CVE ID : CVE-2023-0687**	leo@yuriev.ru/	
Product: gnutls					
Affected Version(s): 3.6.8-11.el8_2					
Observable Discrepancy	15-Feb-2023	7.5	A timing side-channel in the handling of RSA ClientKeyExchange messages was discovered in GnuTLS. This side-channel can be sufficient to recover the key encrypted in the RSA ciphertext across a network in a Bleichenbacher style attack. To achieve a successful decryption the attacker would need to send a large amount of specially crafted messages to the vulnerable server. By recovering the secret	https://gitlab.com/gnutls/gnutls/-/issues/1050, https://github.com/tlsfuzzer/tlsfuzzer/pull/679	A-GNU-GNUT-270223/654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from the ClientKeyExchange message, the attacker would be able to decrypt the application data exchanged over that connection. **CVE ID : CVE-2023-0361**		
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 110.0.5481.77					
Access of Resource Using Incompatible Type ('Type Confusion')	07-Feb-2023	8.8	Type confusion in V8 in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-0696**	https://chromereleases.googleblog.com/2023/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-270223/655
Out-of-bounds Read	07-Feb-2023	8.8	Out of bounds read in WebRTC in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-0698**	https://chromereleases.googleblog.com/2023/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-270223/656
Use After Free	07-Feb-2023	8.8	Use after free in GPU in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page and	https://chromereleases.googleblog.com/2023/02/stable-channel-update-for-	A-GOO-CHRO-270223/657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			browser shutdown. (Chromium security severity: Medium) **CVE ID : CVE-2023-0699**	desktop.html, https://crbug.com/1371859	
Out-of-bounds Write	07-Feb-2023	8.8	Heap buffer overflow in WebUI in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via UI interaction . (Chromium security severity: Medium) **CVE ID : CVE-2023-0701**	https://chromereleases.googleblog.com/2023/02/stable-channel-update-for-desktop.html, https://crbug.com/1405123	A-GOO-CHRO-270223/658
Access of Resource Using Incompatible Type ('Type Confusion')	07-Feb-2023	8.8	Type confusion in Data Transfer in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-0702**	https://chromereleases.googleblog.com/2023/02/stable-channel-update-for-desktop.html, https://crbug.com/1316301	A-GOO-CHRO-270223/659
Access of Resource Using Incompatible Type ('Type Confusion')	07-Feb-2023	8.8	Type confusion in DevTools in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who convinced a user to engage in specific UI	https://chromereleases.googleblog.com/2023/02/stable-channel-update-for-	A-GOO-CHRO-270223/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interactions to potentially exploit heap corruption via UI interactions. (Chromium security severity: Medium) **CVE ID : CVE-2023-0703**	desktop.html, https://crbug.com/1405574	
Integer Overflow or Wraparound	07-Feb-2023	7.5	Integer overflow in Core in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who had one a race condition to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-0705**	https://chromereleases.googleblog.com/2023/02/stable-channel-update-for-desktop.html, https://crbug.com/1238642	A-GOO-CHRO-270223/661
N/A	07-Feb-2023	6.5	Inappropriate implementation in Full screen mode in Google Chrome on Android prior to 110.0.5481.77 allowed a remote attacker to spoof the contents of the security UI via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-0697**	https://chromereleases.googleblog.com/2023/02/stable-channel-update-for-desktop.html, https://crbug.com/1341541	A-GOO-CHRO-270223/662
N/A	07-Feb-2023	6.5	Inappropriate implementation in Download in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to potentially spoof the contents of the Omnibox (URL bar) via	https://chromereleases.googleblog.com/2023/02/stable-channel-update-for-desktop.html,	A-GOO-CHRO-270223/663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-0700**	https://crbug.com/1393732	
N/A	07-Feb-2023	6.5	Insufficient policy enforcement in DevTools in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to bypass same origin policy and proxy settings via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-0704**	https://chromereleases.googleblog.com/2023/02/stable-channel-update-for-desktop.html, https://crbug.com/1385982	A-GOO-CHRO-270223/664
Vendor: gpac					
Product: gpac					
Affected Version(s): * Up to (excluding) 2.2.0					
Stack-based Buffer Overflow	09-Feb-2023	7.8	Stack-based Buffer Overflow in GitHub repository gpac/gpac prior to 2.2. **CVE ID : CVE-2023-0770**	https://github.com/gpac/gpac/commit/c31941822ee275a35bc148382baffef1c53ec1c26, https://huntr.dev/bounties/e0fdeee5-7909-446e-9bd0-db80fd80e8dd	A-GPA-GPAC-270223/665
Affected Version(s): * Up to (excluding) 2.3.0-dev					
Out-of-bounds Read	13-Feb-2023	7.8	Buffer Over-read in GitHub repository gpac/gpac prior to v2.3.0-DEV.	https://github.com/gpac/gpac/commit/be9f8d39	A-GPA-GPAC-270223/666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0817	5bbd196e3812e9cd80708f06bcc206f7, https://hunter.dev/bounties/cb730bc5-d79c-4de6-9e57-10e8c3ce2cf3	
Out-of-bounds Write	13-Feb-2023	7.8	Heap-based Buffer Overflow in GitHub repository gpac/gpac prior to v2.3.0-DEV. **CVE ID : CVE-2023-0819**	https://github.com/gpac/gpac/commit/d067ab3ccdeaa340e8c045a0fd5bcfc22b809e8f, https://hunter.dev/bounties/35793610-dccc-46c8-9f55-6a24c621e4ef	A-GPA-GPAC-270223/667
Off-by-one Error	13-Feb-2023	5.5	Off-by-one Error in GitHub repository gpac/gpac prior to v2.3.0-DEV. **CVE ID : CVE-2023-0818**	https://github.com/gpac/gpac/commit/377ab25f3e502db2934a9cf4b54739e1c89a02ff, https://hunter.dev/bounties/038e7472-f3e9-46c2-9aea-d6dafb62a18a	A-GPA-GPAC-270223/668
Affected Version(s): * Up to (excluding) 2023-02-09					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	09-Feb-2023	7.8	Heap-based Buffer Overflow in GitHub repository gpac/gpac prior to V2.1.0-DEV. **CVE ID : CVE-2023-0760**	https://huntr.dev/bounties/d06223df-a473-4c82-96d0-23726b844b21, https://github.com/gpac/gpac/commit/ea7395f39f601a7750d48d606e9d10ea0b7beefe	A-GPA-GPAC-270223/669
Affected Version(s): 2.3-dev-rev40-g3602a5ded					
Out-of-bounds Write	15-Feb-2023	8.8	A vulnerability, which was classified as critical, has been found in GPAC 2.3-DEV-rev40-g3602a5ded. This issue affects the function mp3_dmx_process of the file filters/reframe_mp3.c. The manipulation leads to heap-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221087. **CVE ID : CVE-2023-0841**	N/A	A-GPA-GPAC-270223/670
Vendor: gptaipower					
Product: gpt_ai_power					
Affected Version(s): * Up to (excluding) 1.4.38					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	13-Feb-2023	4.3	The GPT AI Power: Content Writer & ChatGPT & Image Generator & WooCommerce Product Writer & AI Training WordPress plugin before 1.4.38 does not perform any kind of nonce or privilege checks before letting logged-in users modify arbitrary posts. **CVE ID : CVE-2023-0405**	N/A	A-GPT-GPT_-270223/671
Vendor: gss-ntlmssp_project					
Product: gss-ntlmssp					
Affected Version(s): * Up to (excluding) 1.2.0					
Out-of-bounds Write	14-Feb-2023	8.2	GSS-NTLMSSP is a mechglue plugin for the GSSAPI library that implements NTLM authentication. Prior to version 1.2.0, memory corruption can be triggered when decoding UTF16 strings. The variable `outlen` was not initialized and could cause writing a zero to an arbitrary place in memory if `ntlm_str_convert()` were to fail, which would leave `outlen` uninitialized. This can lead to a denial of service if the write hits unmapped memory or randomly corrupts a byte in the application	https://github.com/gssapi/gss-ntlmssp/commit/c753000eb31835c0664e528fbc99378ae0cbe950	A-GSS-GSS--270223/672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory space. This vulnerability can trigger an out-of-bounds write, leading to memory corruption. This vulnerability can be triggered via the main `gss_accept_sec_context` entry point. This issue is fixed in version 1.2.0. **CVE ID : CVE-2023-25564**		
Out-of-bounds Read	14-Feb-2023	7.5	GSS-NTLMSSP is a mechglue plugin for the GSSAPI library that implements NTLM authentication. Prior to version 1.2.0, multiple out-of-bounds reads when decoding NTLM fields can trigger a denial of service. A 32-bit integer overflow condition can lead to incorrect checks of consistency of length of internal buffers. Although most applications will error out before accepting a singe input buffer of 4GB in length this could theoretically happen. This vulnerability can be triggered via the main `gss_accept_sec_context` entry point if the application allows tokens greater than 4GB in length. This can lead to a large, up to	https://github.com/gssapi/gss-ntlmssp/commit/97c62c6167299028d80765080e74d91dfc99efbd	A-GSS-GSS--270223/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			65KB, out-of-bounds read which could cause a denial-of-service if it reads from unmapped memory. Version 1.2.0 contains a patch for the out-of-bounds reads. **CVE ID : CVE-2023-25563**		
Release of Invalid Pointer or Reference	14-Feb-2023	7.5	GSS-NTLMSSP is a mechglue plugin for the GSSAPI library that implements NTLM authentication. Prior to version 1.2.0, an incorrect free when decoding target information can trigger a denial of service. The error condition incorrectly assumes the `cb` and `sh` buffers contain a copy of the data that needs to be freed. However, that is not the case. This vulnerability can be triggered via the main `gss_accept_sec_context` entry point. This will likely trigger an assertion failure in `free`, causing a denial-of-service. This issue is fixed in version 1.2.0. **CVE ID : CVE-2023-25565**	https://github.com/gssapi/gss-ntlmssp/commit/c16100f60907a2de92bcb676f303b81facee0f64	A-GSS-GSS--270223/674
Missing Release of Memory after	14-Feb-2023	7.5	GSS-NTLMSSP is a mechglue plugin for the GSSAPI library that implements NTLM authentication. Prior to version 1.2.0, a memory	https://github.com/gssapi/gss-ntlmssp/commit/8660fb16474054e	A-GSS-GSS--270223/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			leak can be triggered when parsing usernames which can trigger a denial-of-service. The domain portion of a username may be overridden causing an allocated memory area the size of the domain name to be leaked. An attacker can leak memory via the main `gss_accept_sec_context` entry point, potentially causing a denial-of-service. This issue is fixed in version 1.2.0. **CVE ID : CVE-2023-25566**	692a596e9c79670cd4d3954f4	
Out-of-bounds Read	14-Feb-2023	7.5	GSS-NTLMSSP, a mechglue plugin for the GSSAPI library that implements NTLM authentication, has an out-of-bounds read when decoding target information prior to version 1.2.0. The length of the `av_pair` is not checked properly for two of the elements which can trigger an out-of-bound read. The out-of-bounds read can be triggered via the main `gss_accept_sec_context` entry point and could cause a denial-of-service if the memory is unmapped. The issue is fixed in version 1.2.0.	https://github.com/gssapi/gss-ntlmssp/commit/025fbb756d44ffee8f847db4222ed6aa4bd1fbe4	A-GSS-GSS--270223/676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25567		
Vendor: hapi					
Product: formula					
Affected Version(s): * Up to (excluding) 3.0.1					
N/A	08-Feb-2023	6.5	formula is a math and string formula parser. In versions prior to 3.0.1 crafted user-provided strings to formula's parser might lead to polynomial execution time and a denial of service. Users should upgrade to 3.0.1+. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-25166**	https://github.com/hapijs/formula/security/advisories/GHSA-c2jc-4fpr-4vhg, https://github.com/hapijs/formula/commit/9fbc20a02d75ae809c37a610a57802cd1b41b3fe	A-HAP-FORM-270223/677
Vendor: happyforms					
Product: happyforms					
Affected Version(s): * Up to (excluding) 1.22.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The Happyforms WordPress plugin before 1.22.0 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0096**	N/A	A-HAP-HAPP-270223/678
Vendor: Haproxy					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: haproxy					
Affected Version(s): * Up to (excluding) 2.0.31					
N/A	14-Feb-2023	9.1	HAProxy before 2.7.3 may allow a bypass of access control because HTTP/1 headers are inadvertently lost in some situations, aka "request smuggling." The HTTP header parsers in HAProxy may accept empty header field names, which could be used to truncate the list of HTTP headers and thus make some headers disappear after being parsed and processed for HTTP/1.0 and HTTP/1.1. For HTTP/2 and HTTP/3, the impact is limited because the headers disappear before being parsed and processed, as if they had not been sent by the client. The fixed versions are 2.7.3, 2.6.9, 2.5.12, 2.4.22, 2.2.29, and 2.0.31. **CVE ID : CVE-2023-25725**	https://git.haproxy.org/?p=haproxy-2.7.git;a=commit;h=a0e561ad7f29ed50c473f5a9da664267b60d1112	A-HAP-HAPR-270223/679
Affected Version(s): From (including) 2.1.0 Up to (excluding) 2.2.29					
N/A	14-Feb-2023	9.1	HAProxy before 2.7.3 may allow a bypass of access control because HTTP/1 headers are inadvertently lost in some situations, aka "request smuggling." The HTTP header	https://git.haproxy.org/?p=haproxy-2.7.git;a=commit;h=a0e561ad7f29ed50c473f5a	A-HAP-HAPR-270223/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsers in HAProxy may accept empty header field names, which could be used to truncate the list of HTTP headers and thus make some headers disappear after being parsed and processed for HTTP/1.0 and HTTP/1.1. For HTTP/2 and HTTP/3, the impact is limited because the headers disappear before being parsed and processed, as if they had not been sent by the client. The fixed versions are 2.7.3, 2.6.9, 2.5.12, 2.4.22, 2.2.29, and 2.0.31. **CVE ID : CVE-2023-25725**	9da664267b60d1112	
Affected Version(s): From (including) 2.3.0 Up to (excluding) 2.4.22					
N/A	14-Feb-2023	9.1	HAProxy before 2.7.3 may allow a bypass of access control because HTTP/1 headers are inadvertently lost in some situations, aka "request smuggling." The HTTP header parsers in HAProxy may accept empty header field names, which could be used to truncate the list of HTTP headers and thus make some headers disappear after being parsed and processed for HTTP/1.0 and HTTP/1.1. For HTTP/2	https://git.haproxy.org/?p=haproxy-2.7.git;a=commit;h=a0e561ad7f29ed50c473f5a9da664267b60d1112	A-HAP-HAPR-270223/681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and HTTP/3, the impact is limited because the headers disappear before being parsed and processed, as if they had not been sent by the client. The fixed versions are 2.7.3, 2.6.9, 2.5.12, 2.4.22, 2.2.29, and 2.0.31. **CVE ID : CVE-2023-25725**		
Affected Version(s): From (including) 2.5.0 Up to (excluding) 2.5.12					
N/A	14-Feb-2023	9.1	HAProxy before 2.7.3 may allow a bypass of access control because HTTP/1 headers are inadvertently lost in some situations, aka "request smuggling." The HTTP header parsers in HAProxy may accept empty header field names, which could be used to truncate the list of HTTP headers and thus make some headers disappear after being parsed and processed for HTTP/1.0 and HTTP/1.1. For HTTP/2 and HTTP/3, the impact is limited because the headers disappear before being parsed and processed, as if they had not been sent by the client. The fixed versions are 2.7.3, 2.6.9, 2.5.12, 2.4.22, 2.2.29, and 2.0.31.	https://git.haproxy.org/?p=haproxy-2.7.git;a=commit;h=a0e561ad7f29ed50c473f5a9da664267b60d1112	A-HAP-HAPR-270223/682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25725		
Affected Version(s): From (including) 2.6.0 Up to (excluding) 2.6.9					
N/A	14-Feb-2023	9.1	HAProxy before 2.7.3 may allow a bypass of access control because HTTP/1 headers are inadvertently lost in some situations, aka "request smuggling." The HTTP header parsers in HAProxy may accept empty header field names, which could be used to truncate the list of HTTP headers and thus make some headers disappear after being parsed and processed for HTTP/1.0 and HTTP/1.1. For HTTP/2 and HTTP/3, the impact is limited because the headers disappear before being parsed and processed, as if they had not been sent by the client. The fixed versions are 2.7.3, 2.6.9, 2.5.12, 2.4.22, 2.2.29, and 2.0.31. **CVE ID : CVE-2023-25725**	https://git.haproxy.org/?p=haproxy-2.7.git;a=commit;h=a0e561ad7f29ed50c473f5a9da664267b60d1112	A-HAP-HAPR-270223/683
Affected Version(s): From (including) 2.7.0 Up to (excluding) 2.7.3					
N/A	14-Feb-2023	9.1	HAProxy before 2.7.3 may allow a bypass of access control because HTTP/1 headers are inadvertently lost in some situations, aka "request smuggling."	https://git.haproxy.org/?p=haproxy-2.7.git;a=commit;h=a0e561ad7f29ed50c473f5a	A-HAP-HAPR-270223/684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The HTTP header parsers in HAProxy may accept empty header field names, which could be used to truncate the list of HTTP headers and thus make some headers disappear after being parsed and processed for HTTP/1.0 and HTTP/1.1. For HTTP/2 and HTTP/3, the impact is limited because the headers disappear before being parsed and processed, as if they had not been sent by the client. The fixed versions are 2.7.3, 2.6.9, 2.5.12, 2.4.22, 2.2.29, and 2.0.31. **CVE ID : CVE-2023-25725**	9da664267b60d1112	
Vendor: harfbuzz_project					
Product: harfbuzz					
Affected Version(s): * Up to (including) 6.0.0					
Allocation of Resources Without Limits or Throttling	04-Feb-2023	7.5	hb-ot-layout-gsubgpos.hh in HarfBuzz through 6.0.0 allows attackers to trigger O(n^2) growth via consecutive marks during the process of looking back for base glyphs when attaching marks. **CVE ID : CVE-2023-25193**	https://github.com/harfbuzz/harfbuzz/commit/85be877925ddbf34f74a1229f3ca1716bb6170dc, https://chromium.googlesource.com/chromium/src/+/e1f324aa681af54101c1f2d173	A-HAR-HARF-270223/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				d92adb80e37088/DEPS#361	
Vendor: hashicorp					
Product: boundary					
Affected Version(s): From (including) 0.10.0 Up to (excluding) 0.12.0					
Missing Encryption of Sensitive Data	08-Feb-2023	7.1	HashiCorp Boundary from 0.10.0 through 0.11.2 contain an issue where when using a PKI-based worker with a Key Management Service (KMS) defined in the configuration file, new credentials created after an automatic rotation may not have been encrypted via the intended KMS. This would result in the credentials being stored in plaintext on the Boundary PKI worker's disk. This issue is fixed in version 0.12.0. **CVE ID : CVE-2023-0690**	https://discuss.hashicorp.com/t/hcsec-2023-03-boundary-workers-store-rotated-credentials-in-plaintext-even-when-key-management-service-configured/49907	A-HAS-BOUN-270223/686
Vendor: helm					
Product: helm					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.11.1					
Exposure of Sensitive Information to an Unauthorized Actor	08-Feb-2023	4.3	Helm is a tool that streamlines installing and managing Kubernetes applications.`getHostByName` is a Helm template function introduced in Helm v3. The function is able to accept a hostname and return an IP address for	https://github.com/helm/helm/commit/5abcf74227bfe8e5a3dbf105fe62e7b12deb58d2, https://github.com/helm/helm/sec	A-HEL-HELM-270223/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that hostname. To get the IP address the function performs a DNS lookup. The DNS lookup happens when used with `helm install|upgrade|template` or when the Helm SDK is used to render a chart. Information passed into the chart can be disclosed to the DNS servers used to lookup the IP address. For example, a malicious chart could inject `getHostByName` into a chart in order to disclose values to a malicious DNS server. The issue has been fixed in Helm 3.11.1. Prior to using a chart with Helm verify the `getHostByName` function is not being used in a template to disclose any information you do not want passed to DNS servers. **CVE ID : CVE-2023-25165**	urity/advisories/GHSA-pwcw-6f5g-gxf8	
Vendor: IBM					
Product: cloud_pak_for_business_automation					
Affected Version(s): 21.0.1					
N/A	01-Feb-2023	3.3	IBM ICP4A - Automation Decision Services 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2,	https://www.ibm.com/support/pages/node/6857999	A-IBM-CLOU-270223/688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.0.3, 22.0.1, and 22.0.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 244504. **CVE ID : CVE-2023-23469**		
Affected Version(s): 21.0.2					
N/A	01-Feb-2023	3.3	IBM ICP4A - Automation Decision Services 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 244504. **CVE ID : CVE-2023-23469**	https://www.ibm.com/support/pages/node/6857999	A-IBM-CLOU-270223/689
Affected Version(s): 21.0.3					
N/A	01-Feb-2023	3.3	IBM ICP4A - Automation Decision Services 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 244504. **CVE ID : CVE-2023-23469**	https://www.ibm.com/support/pages/node/6857999	A-IBM-CLOU-270223/690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 22.0.2					
N/A	01-Feb-2023	3.3	IBM ICP4A - Automation Decision Services 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 244504. **CVE ID : CVE-2023-23469**	https://www.ibm.com/support/pages/node/6857999	A-IBM-CLOU-270223/691
Affected Version(s): From (including) 18.0.0 Up to (including) 20.0.3					
N/A	01-Feb-2023	3.3	IBM ICP4A - Automation Decision Services 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 244504. **CVE ID : CVE-2023-23469**	https://www.ibm.com/support/pages/node/6857999	A-IBM-CLOU-270223/692
Product: infosphere_information_server					
Affected Version(s): 11.7					
Improper Neutralization of Input During Web Page Generation	08-Feb-2023	4.6	IBM Infosphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript	https://www.ibm.com/support/pages/node/6890711	A-IBM-INFO-270223/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 245423. **CVE ID : CVE-2023-23475**		
Product: websphere_application_server					
Affected Version(s): 8.5					
Improper Control of Generation of Code ('Code Injection')	03-Feb-2023	9.8	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system with a specially crafted sequence of serialized objects. IBM X-Force ID: 245513. **CVE ID : CVE-2023-23477**	https://www.ibm.com/support/pages/node/6891111, https://exchange.xforce.ibmcloud.com/vulnerabilities/245513	A-IBM-WEBS-270223/694
Affected Version(s): 9.0					
Improper Control of Generation of Code ('Code Injection')	03-Feb-2023	9.8	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system with a specially crafted sequence of serialized objects. IBM X-Force ID: 245513. **CVE ID : CVE-2023-23477**	https://www.ibm.com/support/pages/node/6891111, https://exchange.xforce.ibmcloud.com/vulnerabilities/245513	A-IBM-WEBS-270223/695
Vendor: ichiranusa					
Product: ichiran					
Affected Version(s): * Up to (excluding) 3.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	13-Feb-2023	5.9	Ichiran App for iOS versions prior to 3.1.0 and Ichiran App for Android versions prior to 3.1.0 improperly verify server certificates, which may allow a remote unauthenticated attacker to eavesdrop on an encrypted communication via a man-in-the-middle attack. **CVE ID : CVE-2023-22367**	N/A	A-ICH-ICHI-270223/696
Vendor: in2code					
Product: femanager					
Affected Version(s): * Up to (excluding) 5.5.3					
Missing Authentication for Critical Function	02-Feb-2023	7.5	An issue was discovered in the femanager extension before 5.5.3, 6.x before 6.3.4, and 7.x before 7.1.0 for TYPO3. Missing access checks in the InvitationController allow an unauthenticated user to set the password of all frontend users. **CVE ID : CVE-2023-25013**	https://typo3.org/security/advisory/typo3-ext-sa-2023-001	A-IN2-FEMA-270223/697
Missing Authentication for Critical Function	02-Feb-2023	7.5	An issue was discovered in the femanager extension before 5.5.3, 6.x before 6.3.4, and 7.x before 7.1.0 for TYPO3. Missing access checks in the	https://typo3.org/security/advisory/typo3-ext-sa-2023-001	A-IN2-FEMA-270223/698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InvitationController allow an unauthenticated user to delete all frontend users. **CVE ID : CVE-2023-25014**		
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.3.4					
Missing Authentication for Critical Function	02-Feb-2023	7.5	An issue was discovered in the femanager extension before 5.5.3, 6.x before 6.3.4, and 7.x before 7.1.0 for TYPO3. Missing access checks in the InvitationController allow an unauthenticated user to set the password of all frontend users. **CVE ID : CVE-2023-25013**	https://typo3.org/security/advisory/typo3-ext-sa-2023-001	A-IN2-FEMA-270223/699
Missing Authentication for Critical Function	02-Feb-2023	7.5	An issue was discovered in the femanager extension before 5.5.3, 6.x before 6.3.4, and 7.x before 7.1.0 for TYPO3. Missing access checks in the InvitationController allow an unauthenticated user to delete all frontend users. **CVE ID : CVE-2023-25014**	https://typo3.org/security/advisory/typo3-ext-sa-2023-001	A-IN2-FEMA-270223/700
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.1.0					
Missing Authentica	02-Feb-2023	7.5	An issue was discovered in the	https://typo3.org/securi	A-IN2-FEMA-270223/701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion for Critical Function			femanager extension before 5.5.3, 6.x before 6.3.4, and 7.x before 7.1.0 for TYPO3. Missing access checks in the InvitationController allow an unauthenticated user to set the password of all frontend users. **CVE ID : CVE-2023-25013**	ty/advisory/typo3-ext-sa-2023-001	
Missing Authentication for Critical Function	02-Feb-2023	7.5	An issue was discovered in the femanager extension before 5.5.3, 6.x before 6.3.4, and 7.x before 7.1.0 for TYPO3. Missing access checks in the InvitationController allow an unauthenticated user to delete all frontend users. **CVE ID : CVE-2023-25014**	https://typo3.org/security/advisory/typo3-ext-sa-2023-001	A-IN2-FEMA-270223/702
Vendor: interactive_geo_maps_project					
Product: interactive_geo_maps					
Affected Version(s): * Up to (excluding) 1.5.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Feb-2023	5.4	The Interactive Geo Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the action content parameter in versions up to, and including, 1.5.9 due to insufficient input sanitization and output escaping on user	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2861473%40interactive-geo-maps%2Ftru	A-INT-INTE-270223/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied attributes. This makes it possible for authenticated attackers with editor level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-0731**	nk&old=2857078%40interactive-geo-maps%2Ftrunk&sfp_email=&sfph_mail=#file4	
Vendor: inventory_management_system_project					
Product: inventory_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Feb-2023	4.8	A stored cross-site scripting (XSS) vulnerability in the component /php-inventory-management-system/categories.php of Inventory Management System v1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Categories Name parameter. **CVE ID : CVE-2023-24231**	N/A	A-INV-INVE-270223/704
Improper Neutralization of Input During Web Page Generation	10-Feb-2023	4.8	A stored cross-site scripting (XSS) vulnerability in the component /php-inventory-management-system/product.php of Inventory Management System v1 allows	N/A	A-INV-INVE-270223/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Product Name parameter. **CVE ID : CVE-2023-24232**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Feb-2023	4.8	A stored cross-site scripting (XSS) vulnerability in the component /php-inventory-management-system/orders.php?o=add of Inventory Management System v1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Client Name parameter. **CVE ID : CVE-2023-24233**	N/A	A-INV-INVE-270223/706
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Feb-2023	4.8	A stored cross-site scripting (XSS) vulnerability in the component php-inventory-management-system/brand.php of Inventory Management System v1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Brand Name parameter. **CVE ID : CVE-2023-24234**	N/A	A-INV-INVE-270223/707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: invoiceplane					
Product: invoiceplane					
Affected Version(s): 1.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Feb-2023	6.1	Cross Site Scripting (XSS) vulnerability in InvoicePlane 1.6 via filter_product input to file modal_product_lookups.php. **CVE ID : CVE-2023-23011**	N/A	A-INV-INVO-270223/708
Vendor: Ipython					
Product: ipython					
Affected Version(s): * Up to (excluding) 8.10.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Feb-2023	7	IPython (Interactive Python) is a command shell for interactive computing in multiple programming languages, originally developed for the Python programming language. Versions prior to 8.1.0 are subject to a command injection vulnerability with very specific prerequisites. This vulnerability requires that the function `IPython.utils.terminal.set_term_title` be called on Windows in a Python environment where ctypes is not available. The dependency on `ctypes` in `IPython.utils._process_win32` prevents the	https://github.com/ipython/ipython/commit/385d69325319a5972ee9b5983638e3617f21cb1f, https://github.com/ipython/ipython/security/advisories/GHSA-29gw-9793-fvw7	A-IPY-IPYT-270223/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable code from ever being reached in the ipython binary. However, as a library that could be used by another tool `set_term_title` could be called and hence introduce a vulnerability. Should an attacker get untrusted input to an instance of this function they would be able to inject shell commands as current process and limited to the scope of the current process. Users of ipython as a library are advised to upgrade. Users unable to upgrade should ensure that any calls to the `IPython.utils.terminal.set_term_title` function are done with trusted or filtered input. **CVE ID : CVE-2023-24816**		
Vendor: jellyfin					
Product: jellyfin					
Affected Version(s): From (including) 10.8.0 Up to (including) 10.8.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Feb-2023	5.4	In Jellyfin 10.8.x through 10.8.3, the name of a collection is vulnerable to stored XSS. This allows an attacker to steal access tokens from the localStorage of the victim.	N/A	A-JEL-JELL-270223/710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23635		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Feb-2023	5.4	In Jellyfin 10.8.x through 10.8.3, the name of a playlist is vulnerable to stored XSS. This allows an attacker to steal access tokens from the localStorage of the victim. **CVE ID : CVE-2023-23636**	https://github.com/jellyfin/jellyfin-web/issues/3788	A-JEL-JELL-270223/711
Vendor: Jenkins					
Product: azure_credentials					
Affected Version(s): * Up to (excluding) 254.v64da_8176c83a					
Cross-Site Request Forgery (CSRF)	15-Feb-2023	8.8	A cross-site request forgery (CSRF) vulnerability in Jenkins Azure Credentials Plugin 253.v887e0f9e898b and earlier allows attackers to connect to an attacker-specified web server. **CVE ID : CVE-2023-25767**	https://www.jenkins.io/security/advisory/2023-02-15/#SECURITY-1756	A-JEN-AZUR-270223/712
Incorrect Authorization	15-Feb-2023	6.5	A missing permission check in Jenkins Azure Credentials Plugin 253.v887e0f9e898b and earlier allows attackers with Overall/Read permission to connect to an attacker-specified web server. **CVE ID : CVE-2023-25768**	https://www.jenkins.io/security/advisory/2023-02-15/#SECURITY-1756	A-JEN-AZUR-270223/713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	15-Feb-2023	4.3	A missing permission check in Jenkins Azure Credentials Plugin 253.v887e0f9e898b and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. **CVE ID : CVE-2023-25766**	https://www.jenkins.io/security/advisory/2023-02-15/#SECURITY-1757	A-JEN-AZUR-270223/714
Product: email_extension					
Affected Version(s): * Up to (including) 2.93					
Protection Mechanism Failure	15-Feb-2023	9.9	In Jenkins Email Extension Plugin 2.93 and earlier, templates defined inside a folder were not subject to Script Security protection, allowing attackers able to define email templates in folders to bypass the sandbox protection and execute arbitrary code in the context of the Jenkins controller JVM. **CVE ID : CVE-2023-25765**	https://www.jenkins.io/security/advisory/2023-02-15/#SECURITY-2939	A-JEN-EMAI-270223/715
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Feb-2023	5.4	Jenkins Email Extension Plugin 2.93 and earlier does not escape various fields included in bundled email templates, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers	https://www.jenkins.io/security/advisory/2023-02-15/#SECURITY-2931	A-JEN-EMAI-270223/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to control affected fields. **CVE ID : CVE-2023-25763**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Feb-2023	5.4	Jenkins Email Extension Plugin 2.93 and earlier does not escape, sanitize, or sandbox rendered email template output or log output generated during template rendering, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to create or change custom email templates. **CVE ID : CVE-2023-25764**	https://www.jenkins.io/security/advisory/2023-02-15/#SECURITY-2934	A-JEN-EMAI-270223/717
Product: junit					
Affected Version(s): * Up to (including) 1166.va_436e268e972					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Feb-2023	5.4	Jenkins JUnit Plugin 1166.va_436e268e972 and earlier does not escape test case class names in JavaScript expressions, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control test case class names in the JUnit resources processed by the plugin. **CVE ID : CVE-2023-25761**	https://www.jenkins.io/security/advisory/2023-02-15/#SECURITY-3032	A-JEN-JUNI-270223/718
Product: pipeline					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): _build_step Up to (including) 2.18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Feb-2023	5.4	Jenkins Pipeline: Build Step Plugin 2.18 and earlier does not escape job names in a JavaScript expression used in the Pipeline Snippet Generator, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control job names. **CVE ID : CVE-2023-25762**	https://www.jenkins.io/security/advisory/2023-02-15/#SECURITY-3019	A-JEN-PIPE-270223/719
Product: synopsys_coverity					
Affected Version(s): * Up to (excluding) 3.0.3					
Incorrect Default Permissions	15-Feb-2023	4.3	Missing permission checks in Synopsys Jenkins Coverity Plugin 3.0.2 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2023-23848**	https://www.jenkins.io/security/advisory/2023-02-15/#SECURITY-2793%20(2), https://community.synopsys.com/s/article/SIG-Product-Security-Advisory-Multiple-CVEs-affecting-Coverity-Jenkins-Plugin	A-JEN-SYNO-270223/720
Incorrect Default	15-Feb-2023	4.3	A missing permission check in Synopsys	https://www.jenkins.io/	A-JEN-SYNO-270223/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			Jenkins Coverity Plugin 3.0.2 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. **CVE ID : CVE-2023-23850**	security/advisory/2023-02-15/#SECURITY-2793%20(1), https://community.synopsys.com/s/article/SIG-Product-Security-Advisory-Multiple-CVEs-affecting-Coverity-Jenkins-Plugin	
Cross-Site Request Forgery (CSRF)	15-Feb-2023	3.5	A cross-site request forgery (CSRF) vulnerability in Synopsys Jenkins Coverity Plugin 3.0.2 and earlier allows attackers to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2023-23847**	https://www.jenkins.io/security/advisory/2023-02-15/#SECURITY-2793%20(2), https://community.synopsys.com/s/article/SIG-Product-Security-Advisory-Multiple-CVEs-affecting-Coverity-Jenkins-Plugin	A-JEN-SYNO-270223/722
Vendor: jfinaloa_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: jfinaloa					
Affected Version(s): 1.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Feb-2023	9.8	A vulnerability was found in glorylion JFinalOA 1.0.2 and classified as critical. This issue affects some unknown processing of the file src/main/java/com/pointlion/mvc/common/model/SysOrg.java. 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-220469 was assigned to this vulnerability. **CVE ID : CVE-2023-0758**	N/A	A-JFI-JFIN-270223/723
Vendor: jflyfox					
Product: jfinal_cms					
Affected Version(s): 5.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Feb-2023	6.1	jfinal_cms 5.1.0 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-22975**	N/A	A-JFL-JFIN-270223/724
Vendor: Joomla					
Product: joomla\!					
Affected Version(s): From (including) 4.0.0 Up to (including) 4.2.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	01-Feb-2023	4.3	An issue was discovered in Joomla! 4.0.0 through 4.2.4. A missing ACL check allows non super-admin users to access com_actionlogs. **CVE ID : CVE-2023-23751**	https://developer.joomla.org/security-centre/891-20230102-core-missing-acl-checks-for-com-actionlogs.html	A-JOO-JOOM-270223/725
Affected Version(s): From (including) 4.0.0 Up to (including) 4.2.6					
Cross-Site Request Forgery (CSRF)	01-Feb-2023	6.3	An issue was discovered in Joomla! 4.0.0 through 4.2.6. A missing token check causes a CSRF vulnerability in the handling of post-installation messages. **CVE ID : CVE-2023-23750**	https://developer.joomla.org/security-centre/890-20230101-core-csrf-within-post-installation-messages.html	A-JOO-JOOM-270223/726
Vendor: json-parser_project					
Product: json-parser					
Affected Version(s): 1.1.0					
Out-of-bounds Write	03-Feb-2023	9.8	Buffer OverFlow Vulnerability in Barenboim json-parser master and v1.1.0 fixed in v1.1.1 allows an attacker to execute arbitrary code via the json_value_parse function. **CVE ID : CVE-2023-23088**	https://github.com/Barenboim/json-parser/issues/7	A-JSO-JSON-270223/727
Vendor: judge					
Product: product_reviews_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.3.21					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	The Judge.me Product Reviews for WooCommerce WordPress plugin before 1.3.21 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0061**	N/A	A-JUD-PROD-270223/728
Vendor: kardex					
Product: kardex_control_center					
Affected Version(s): 5.7.12\\+0-a203c2a213-master					
Improper Control of Generation of Code ('Code Injection')	15-Feb-2023	9.8	Kardex Mlog MCC 5.7.12+0-a203c2a213-master allows remote code execution. It spawns a web interface listening on port 8088. A user-controllable path is handed to a path-concatenation method (Path.Combine from .NET) without proper sanitisation. This yields the possibility of including local files, as well as remote files on SMB shares. If one provides a file with the extension .t4, it is rendered with the .NET templating	N/A	A-KAR-KARD-270223/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			engine mono/t4, which can execute code. **CVE ID : CVE-2023-22855**		
Vendor: kiwitcms					
Product: kiwi_tcms					
Affected Version(s): * Up to (excluding) 12.0					
Improper Restriction of Excessive Authentication Attempts	15-Feb-2023	9.8	Kiwi TCMS, an open source test management system, does not impose rate limits in versions prior to 12.0. This makes it easier to attempt brute-force attacks against the login page. Users should upgrade to v12.0 or later to receive a patch. As a workaround, users may install and configure a rate-limiting proxy in front of Kiwi TCMS. **CVE ID : CVE-2023-25156**	https://github.com/kiwitcms/Kiwi/security/advisories/GHSA-7968-h4m4-ghm9, https://github.com/kiwitcms/Kiwi/commit/0ed213fa0ddb7a6dc77e3c3b99e8fc90ccdaf46f	A-KIW-KIWI-270223/730
Allocation of Resources Without Limits or Throttling	15-Feb-2023	5.9	Kiwi TCMS, an open source test management system, does not impose rate limits in versions prior to 12.0. This makes it easier to attempt denial-of-service attacks against the Password reset page. An attacker could potentially send a large number of emails if they know the email addresses of users in Kiwi TCMS. Additionally that may strain SMTP	https://github.com/kiwitcms/Kiwi/security/advisories/GHSA-7j9h-3jxf-3vrf, https://github.com/kiwitcms/Kiwi/commit/761305d04f5910ba14cc04d1255a8f1afdbb87f3	A-KIW-KIWI-270223/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resources. Users should upgrade to v12.0 or later to receive a patch. As potential workarounds, users may install and configure a rate-limiting proxy in front of Kiwi TCMS and/or configure rate limits on their email server when possible. **CVE ID : CVE-2023-25171**		
Vendor: Kodi					
Product: kodi					
Affected Version(s): * Up to (including) 19.5					
Out-of-bounds Write	03-Feb-2023	4.6	A heap buffer overflow vulnerability in Kodi Home Theater Software up to 19.5 allows attackers to cause a denial of service due to an improper length of the value passed to the offset argument. **CVE ID : CVE-2023-23082**	https://github.com/fritsch/xbmc/commit/367cc80d66b0310b460f587fea44274b442951f1, https://github.com/xbmc/xbmc/pull/22380, https://github.com/xbmc/xbmc/commit/8c2aafb6d4987833803e037c923aaf83f9ff41e1, https://github.com/xbmc/xbmc/issues/22377	A-KOD-KODI-270223/732
Vendor: kraken					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: kraken.io_image_optimizer					
Affected Version(s): * Up to (including) 2.6.8					
Missing Authorization	01-Feb-2023	6.5	The Kraken.io Image Optimizer plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on its AJAX actions in versions up to, and including, 2.6.8. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to reset image optimizations. **CVE ID : CVE-2023-0619**	N/A	A-KRA-KRAK-270223/733
Vendor: libpeconv_project					
Product: libpeconv					
Affected Version(s): * Up to (excluding) 2022-11-30					
N/A	15-Feb-2023	9.8	Libpeconv – access violation, before commit b076013 (30/11/2022). **CVE ID : CVE-2023-23461**	N/A	A-LIB-LIBP-270223/734
Integer Overflow or Wraparound	15-Feb-2023	9.8	Libpeconv – integer overflow, before commit 75b1565 (30/11/2022). **CVE ID : CVE-2023-23462**	N/A	A-LIB-LIBP-270223/735
Vendor: Libtiff					
Product: libtiff					
Affected Version(s): * Up to (including) 4.4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Feb-2023	5.5	LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in tools/tiffcrop.c:3488, 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 afaabc3e. **CVE ID : CVE-2023-0795**	https://gitlab.com/libtiff/libtiff/-/commit/afaabc3e50d4e5d80a94143f7e3c997e7e410f68, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0795.json, https://gitlab.com/libtiff/libtiff/-/issues/493	A-LIB-LIBT-270223/736
Out-of-bounds Read	13-Feb-2023	5.5	LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in tools/tiffcrop.c:3592, 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 afaabc3e. **CVE ID : CVE-2023-0796**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0796.json, https://gitlab.com/libtiff/libtiff/-/commit/afaabc3e50d4e5d80a94143f7e3c997e7e410f68, https://gitlab.com/libtiff/libtiff/-/issues/499	A-LIB-LIBT-270223/737
Out-of-bounds Read	13-Feb-2023	5.5	LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in libtiff/tif_unix.c:368, invoked by	https://gitlab.com/libtiff/libtiff/-/commit/afaabc3e50d4e	A-LIB-LIBT-270223/738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tools/tiffcrop.c:2903 and tools/tiffcrop.c:6921, 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 afaabc3e. **CVE ID : CVE-2023-0797**	5d80a94143f7e3c997e7e410f68, https://gitlab.com/libtiff/libtiff/-/issues/495, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0797.json	
Out-of-bounds Read	13-Feb-2023	5.5	LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in tools/tiffcrop.c:3400, 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 afaabc3e. **CVE ID : CVE-2023-0798**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0798.json, https://gitlab.com/libtiff/libtiff/-/commit/afaabc3e50d4e5d80a94143f7e3c997e7e410f68, https://gitlab.com/libtiff/libtiff/-/issues/492	A-LIB-LIBT-270223/739
Use After Free	13-Feb-2023	5.5	LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in tools/tiffcrop.c:3701, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0799.json, https://gitlab.com/libtiff/libtiff/-	A-LIB-LIBT-270223/740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			available with commit afaabc3e. **CVE ID : CVE-2023-0799**	/commit/afaabc3e50d4e5d80a94143f7e3c997e7e410f68, https://gitlab.com/libtiff/libtiff/-/issues/494	
Out-of-bounds Write	13-Feb-2023	5.5	LibTIFF 4.4.0 has an out-of-bounds write in tiffcrop in tools/tiffcrop.c:3502, 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 33aee127. **CVE ID : CVE-2023-0800**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0800.json, https://gitlab.com/libtiff/libtiff/-/commit/33aee1275d9d1384791d2206776eb8152d397f00, https://gitlab.com/libtiff/libtiff/-/issues/496	A-LIB-LIBT-270223/741
Out-of-bounds Write	13-Feb-2023	5.5	LibTIFF 4.4.0 has an out-of-bounds write in tiffcrop in libtiff/tif_unix.c:368, invoked by tools/tiffcrop.c:2903 and tools/tiffcrop.c:6778, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is	https://gitlab.com/libtiff/libtiff/-/commit/33aee1275d9d1384791d2206776eb8152d397f00, https://gitlab.com/libtiff/libtiff/-/issues/498, https://gitlab.com/gitlab-org/cves/-	A-LIB-LIBT-270223/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			available with commit 33aee127. **CVE ID : CVE-2023-0801**	/blob/master/2023/CVE-2023-0801.json	
Out-of-bounds Write	13-Feb-2023	5.5	LibTIFF 4.4.0 has an out-of-bounds write in tiffcrop in tools/tiffcrop.c:3724, 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 33aee127. **CVE ID : CVE-2023-0802**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0802.json, https://gitlab.com/libtiff/libtiff/-/issues/500, https://gitlab.com/libtiff/libtiff/-/commit/33aee1275d9d1384791d2206776eb8152d397f00	A-LIB-LIBT-270223/743
Out-of-bounds Write	13-Feb-2023	5.5	LibTIFF 4.4.0 has an out-of-bounds write in tiffcrop in tools/tiffcrop.c:3516, 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 33aee127. **CVE ID : CVE-2023-0803**	https://gitlab.com/libtiff/libtiff/-/issues/501, https://gitlab.com/libtiff/libtiff/-/commit/33aee1275d9d1384791d2206776eb8152d397f00, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0803.json	A-LIB-LIBT-270223/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Feb-2023	5.5	LibTIFF 4.4.0 has an out-of-bounds write in tiffcrop in tools/tiffcrop.c:3609, 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 33aee127. **CVE ID : CVE-2023-0804**	https://gitlab.com/libtiff/libtiff/-/commit/33aee1275d9d1384791d2206776eb8152d397f00, https://gitlab.com/libtiff/libtiff/-/issues/497, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0804.json	A-LIB-LIBT-270223/745
Vendor: lightspeedhq					
Product: ecwid_ecommerce_shopping_cart					
Affected Version(s): * Up to (excluding) 6.11.4					
Cross-Site Request Forgery (CSRF)	14-Feb-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Ecwid Ecommerce Ecwid Ecommerce Shopping Cart plugin <= 6.11.3 versions. **CVE ID : CVE-2023-24377**	N/A	A-LIG-ECWI-270223/746
Vendor: Linuxfoundation					
Product: argo_continuous_delivery					
Affected Version(s): 2.6.0					
Insertion of Sensitive Information into Log File	08-Feb-2023	6.5	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All versions of Argo CD starting with v2.6.0-rc1 have an output	https://github.com/argoproj/argo-cd/pull/12320, https://github.com/argo	A-LIN-ARGO-270223/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sanitization bug which leaks repository access credentials in error messages. These error messages are visible to the user, and they are logged. The error message is visible when a user attempts to create or update an Application via the Argo CD API (and therefor the UI or CLI). The user must have `applications, create` or `applications, update` RBAC access to reach the code which may produce the error. The user is not guaranteed to be able to trigger the error message. They may attempt to spam the API with requests to trigger a rate limit error from the upstream repository. If the user has `repositories, update` access, they may edit an existing repository to introduce a URL typo or otherwise force an error message. But if they have that level of access, they are probably intended to have access to the credentials anyway. A patch for this vulnerability has been released in version 2.6.1. Users are advised to upgrade. There are	proj/argo-cd/security/advisories/GHSA-mv6w-j4xc-qpfw	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			no known workarounds for this vulnerability. **CVE ID : CVE-2023-25163**		
Product: backstage_catalog-model					
Affected Version(s): * Up to (excluding) 1.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	Backstage is an open platform for building developer portals. `@backstage/catalog-model` prior to version 1.2.0, `@backstage/core-components` prior to 0.12.4, and `@backstage/plugin-catalog-backend` prior to 1.7.2 are affected by a cross-site scripting vulnerability. This vulnerability allows a malicious actor with access to add or modify content in an instance of the Backstage software catalog to inject script URLs in the entities stored in the catalog. If users of the catalog then click on said URLs, that can lead to an XSS attack. This vulnerability has been patched in both the frontend and backend implementations. The default `Link` component from `@backstage/core-components` version 1.2.0 and greater will now reject `javascript:` URLs, and there is a	https://github.com/backstage/backstage/security/advisories/GHSA-7hv8-3fr9-j2hv, https://github.com/backstage/backstage/commit/3d1371954512f7fa8bd0e2d357e00eada2c3e8a8	A-LIN-BACK-270223/748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global override of `window.open` to do the same. In addition, the catalog model v0.12.4 and greater as well as the catalog backend v1.7.2 and greater now has additional validation built in that prevents `javascript:` URLs in known annotations. As a workaround, the general practice of limiting access to modifying catalog content and requiring code reviews greatly help mitigate this vulnerability. **CVE ID : CVE-2023-25571**		
Product: backstage_core-components					
Affected Version(s): * Up to (excluding) 0.12.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	Backstage is an open platform for building developer portals. `@backstage/catalog-model` prior to version 1.2.0, `@backstage/core-components` prior to 0.12.4, and `@backstage/plugin-catalog-backend` prior to 1.7.2 are affected by a cross-site scripting vulnerability. This vulnerability allows a malicious actor with access to add or modify content in an instance of the Backstage	https://github.com/backstage/backstage/security/advisories/GHSA-7hv8-3fr9-j2hv, https://github.com/backstage/backstage/commit/3d1371954512f7fa8bd0e2d357e00eada2c3e8a8	A-LIN-BACK-270223/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software catalog to inject script URLs in the entities stored in the catalog. If users of the catalog then click on said URLs, that can lead to an XSS attack. This vulnerability has been patched in both the frontend and backend implementations. The default `Link` component from `@backstage/core-components` version 1.2.0 and greater will now reject `javascript:` URLs, and there is a global override of `window.open` to do the same. In addition, the catalog model v0.12.4 and greater as well as the catalog backend v1.7.2 and greater now has additional validation built in that prevents `javascript:` URLs in known annotations. As a workaround, the general practice of limiting access to modifying catalog content and requiring code reviews greatly help mitigate this vulnerability. **CVE ID : CVE-2023-25571**		
Product: backstage_plugin-catalog-backend					
Affected Version(s): * Up to (excluding) 1.7.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	Backstage is an open platform for building developer portals. `@backstage/catalog-model` prior to version 1.2.0, `@backstage/core-components` prior to 0.12.4, and `@backstage/plugin-catalog-backend` prior to 1.7.2 are affected by a cross-site scripting vulnerability. This vulnerability allows a malicious actor with access to add or modify content in an instance of the Backstage software catalog to inject script URLs in the entities stored in the catalog. If users of the catalog then click on said URLs, that can lead to an XSS attack. This vulnerability has been patched in both the frontend and backend implementations. The default `Link` component from `@backstage/core-components` version 1.2.0 and greater will now reject `javascript:` URLs, and there is a global override of `window.open` to do the same. In addition, the catalog model v0.12.4 and greater as well as the catalog backend v1.7.2 and	https://github.com/backstage/backstage/security/advisories/GHSA-7hv8-3fr9-j2hv, https://github.com/backstage/backstage/commit/3d1371954512f7fa8bd0e2d357e00eada2c3e8a8	A-LIN-BACK-270223/750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			greater now has additional validation built in that prevents `javascript:` URLs in known annotations. As a workaround, the general practice of limiting access to modifying catalog content and requiring code reviews greatly help mitigate this vulnerability. **CVE ID : CVE-2023-25571**		
Vendor: ljapps					
Product: wp_airbnb_review_slider					
Affected Version(s): * Up to (excluding) 3.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Feb-2023	8.8	The WP Airbnb Review Slider WordPress plugin before 3.3 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as subscriber. **CVE ID : CVE-2023-0262**	N/A	A-LJA-WP_A-270223/751
Product: wp_google_review_slider					
Affected Version(s): * Up to (excluding) 11.8					
Improper Neutralization of Special Elements used in an SQL Command	13-Feb-2023	8.8	The WP Google Review Slider WordPress plugin before 11.8 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection	N/A	A-LJA-WP_G-270223/752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			exploitable by users with a role as low as subscriber. **CVE ID : CVE-2023-0259**		
Product: wp_review_slider					
Affected Version(s): * Up to (excluding) 12.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Feb-2023	8.8	The WP Review Slider WordPress plugin before 12.2 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as subscriber. **CVE ID : CVE-2023-0260**	N/A	A-LJA-WP_R-270223/753
Product: wp_tripadvisor_review_slider					
Affected Version(s): * Up to (excluding) 10.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Feb-2023	8.8	The WP TripAdvisor Review Slider WordPress plugin before 10.8 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as subscriber. **CVE ID : CVE-2023-0261**	N/A	A-LJA-WP_T-270223/754
Product: wp_yelp_review_slider					
Affected Version(s): * Up to (excluding) 7.1					
Improper Neutralizat	13-Feb-2023	8.8	The WP Yelp Review Slider WordPress	N/A	A-LJA-WP_Y-270223/755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			plugin before 7.1 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as subscriber. **CVE ID : CVE-2023-0263**		
Vendor: lmxcms					
Product: lmxcms					
Affected Version(s): 1.41					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Feb-2023	6.5	lmxcms v1.41 was discovered to contain an arbitrary file deletion vulnerability via BackdbAction.class.php. **CVE ID : CVE-2023-23136**	N/A	A-LMX-LMXC-270223/756
Vendor: mage-people					
Product: event_manager_and_tickets_selling_for_woocommerce					
Affected Version(s): * Up to (excluding) 3.8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The Event Manager and Tickets Selling Plugin for WooCommerce WordPress plugin before 3.8.0 does not validate and escape some of its post meta before outputting them back in a page/post, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	N/A	A-MAG-EVEN-270223/757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0144		
Vendor: marmelab					
Product: ra-ui-materialui					
Affected Version(s): * Up to (excluding) 3.9.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	react-admin is a frontend framework for building browser applications on top of REST/GraphQL APIs. react-admin prior to versions 3.19.12 and 4.7.6, along with ra-ui-materialui prior to 3.19.12 and 4.7.6, are vulnerable to cross-site scripting. All React applications built with react-admin and using the `<RichTextField>` are affected. `<RichTextField>` outputs the field value using `dangerouslySetInnerHTML` without client-side sanitization. If the data isn't sanitized server-side, this opens a possible cross-site scripting (XSS) attack. Versions 3.19.12 and 4.7.6 now use `DOMPurify` to escape the HTML before outputting it with React and `dangerouslySetInnerHTML`. Users who already sanitize HTML data server-side do not need to upgrade. As a workaround, users may	https://github.com/marmelab/react-admin/pull/8645, https://github.com/marmelab/react-admin/pull/8644, https://github.com/marmelab/react-admin/security/advisories/GHSA-5jcr-82fh-339v	A-MAR-RA-U-270223/758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			replace the `<RichTextField>` by a custom field doing sanitization by hand. **CVE ID : CVE-2023-25572**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.7.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	react-admin is a frontend framework for building browser applications on top of REST/GraphQL APIs. react-admin prior to versions 3.19.12 and 4.7.6, along with ra-ui-materialui prior to 3.19.12 and 4.7.6, are vulnerable to cross-site scripting. All React applications built with react-admin and using the `<RichTextField>` are affected. `<RichTextField>` outputs the field value using `dangerouslySetInnerHTML` without client-side sanitization. If the data isn't sanitized server-side, this opens a possible cross-site scripting (XSS) attack. Versions 3.19.12 and 4.7.6 now use `DOMPurify` to escape the HTML before outputting it with React and `dangerouslySetInnerHTML`. Users who already sanitize HTML data server-side do not	https://github.com/marmelab/react-admin/pull/8645, https://github.com/marmelab/react-admin/pull/8644, https://github.com/marmelab/react-admin/security/advisories/GHSA-5jcr-82fh-339v	A-MAR-RA-U-270223/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			need to upgrade. As a workaround, users may replace the `<RichTextField>` by a custom field doing sanitization by hand. **CVE ID : CVE-2023-25572**		
Product: react-admin					
Affected Version(s): * Up to (excluding) 3.9.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	react-admin is a frontend framework for building browser applications on top of REST/GraphQL APIs. react-admin prior to versions 3.19.12 and 4.7.6, along with ra-ui-materialui prior to 3.19.12 and 4.7.6, are vulnerable to cross-site scripting. All React applications built with react-admin and using the `<RichTextField>` are affected. `<RichTextField>` outputs the field value using `dangerouslySetInnerHTML` without client-side sanitization. If the data isn't sanitized server-side, this opens a possible cross-site scripting (XSS) attack. Versions 3.19.12 and 4.7.6 now use `DOMPurify` to escape the HTML before outputting it with React and `dangerouslySetInnerH	https://github.com/marmelab/react-admin/pull/8645, https://github.com/marmelab/react-admin/pull/8644, https://github.com/marmelab/react-admin/security/advisories/GHSA-5jcr-82fh-339v	A-MAR-REAC-270223/760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TML`. Users who already sanitize HTML data server-side do not need to upgrade. As a workaround, users may replace the `<RichTextField>` by a custom field doing sanitization by hand. **CVE ID : CVE-2023-25572**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.7.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	react-admin is a frontend framework for building browser applications on top of REST/GraphQL APIs. react-admin prior to versions 3.19.12 and 4.7.6, along with ra-ui-materialui prior to 3.19.12 and 4.7.6, are vulnerable to cross-site scripting. All React applications built with react-admin and using the `<RichTextField>` are affected. `<RichTextField>` outputs the field value using `dangerouslySetInnerHTML` without client-side sanitization. If the data isn't sanitized server-side, this opens a possible cross-site scripting (XSS) attack. Versions 3.19.12 and 4.7.6 now use `DOMPurify` to escape the HTML before outputting it with React	https://github.com/marmelab/react-admin/pull/8645, https://github.com/marmelab/react-admin/pull/8644, https://github.com/marmelab/react-admin/security/advisories/GHSA-5jcr-82fh-339v	A-MAR-REAC-270223/761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and `dangerouslySetInnerHTML`. Users who already sanitize HTML data server-side do not need to upgrade. As a workaround, users may replace the `<RichTextField>` by a custom field doing sanitization by hand. **CVE ID : CVE-2023-25572**		
Vendor: material_design_icons_for_page_builders_project					
Product: material_design_icons_for_page_builders					
Affected Version(s): * Up to (excluding) 1.4.3					
Cross-Site Request Forgery (CSRF)	14-Feb-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Photon WP Material Design Icons for Page Builders plugin <= 1.4.2 versions. **CVE ID : CVE-2023-24382**	N/A	A-MAT-MATE-270223/762
Vendor: mediacp					
Product: media_control_panel					
Affected Version(s): 2.13.1					
Cross-Site Request Forgery (CSRF)	15-Feb-2023	8.8	Media CP Media Control Panel latest version. CSRF possible through unspecified endpoint. **CVE ID : CVE-2023-23465**	N/A	A-MED-MEDI-270223/763
N/A	15-Feb-2023	7.5	Media CP Media Control Panel latest version. A Permissive Flash Cross-domain Policy may allow information disclosure.	N/A	A-MED-MEDI-270223/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23464		
Insufficiently Protected Credentials	15-Feb-2023	7.5	Media CP Media Control Panel latest version. Insufficiently protected credential change. **CVE ID : CVE-2023-23466**	N/A	A-MED-MEDI-270223/765
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Feb-2023	6.1	Media CP Media Control Panel latest version. Reflected XSS possible through unspecified endpoint. **CVE ID : CVE-2023-23467**	N/A	A-MED-MEDI-270223/766
Vendor: medical_certificate_generator_app_project					
Product: medical_certificate_generator_app					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Feb-2023	9.8	A vulnerability was found in SourceCodester Medical Certificate Generator App 1.0. It has been rated as critical. Affected by this issue is the function delete_record of the file function.php. The manipulation of the argument id leads to sql injection. VDB-220346 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0707**	N/A	A-MED-MEDI-270223/767
Improper Neutralization of	10-Feb-2023	9.8	A vulnerability has been found in SourceCodester Medical	N/A	A-MED-MEDI-270223/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			Certificate Generator App 1.0 and classified as critical. This vulnerability affects unknown code of the file action.php. The manipulation of the argument lastname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-220558 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0774**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Feb-2023	8.8	A vulnerability, which was classified as critical, has been found in SourceCodester Medical Certificate Generator App 1.0. Affected by this issue is some unknown functionality of the file manage_record.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The identifier of this vulnerability is VDB-220340. **CVE ID : CVE-2023-0706**	N/A	A-MED-MEDI-270223/769
Vendor: mendix					
Product: mendix					
Affected Version(s): From (including) 7.0.2 Up to (excluding) 7.23.34					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	14-Feb-2023	7.5	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.34), Mendix Applications using Mendix 8 (All versions < V8.18.23), Mendix Applications using Mendix 9 (All versions < V9.22.0), Mendix Applications using Mendix 9 (V9.12) (All versions < V9.12.10), Mendix Applications using Mendix 9 (V9.18) (All versions < V9.18.4), Mendix Applications using Mendix 9 (V9.6) (All versions < V9.6.15). Some of the Mendix runtime API's allow attackers to bypass XPath constraints and retrieve information using XPath queries that trigger errors. **CVE ID : CVE-2023-23835**	N/A	A-MEN-MEND-270223/770
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.18.23					
Improper Access Control	14-Feb-2023	7.5	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.34), Mendix Applications using Mendix 8 (All versions < V8.18.23), Mendix Applications using Mendix 9 (All versions < V9.22.0), Mendix Applications	N/A	A-MEN-MEND-270223/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using Mendix 9 (V9.12) (All versions < V9.12.10), Mendix Applications using Mendix 9 (V9.18) (All versions < V9.18.4), Mendix Applications using Mendix 9 (V9.6) (All versions < V9.6.15). Some of the Mendix runtime API's allow attackers to bypass XPath constraints and retrieve information using XPath queries that trigger errors. **CVE ID : CVE-2023-23835**		
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.6.15					
Improper Access Control	14-Feb-2023	7.5	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.34), Mendix Applications using Mendix 8 (All versions < V8.18.23), Mendix Applications using Mendix 9 (All versions < V9.22.0), Mendix Applications using Mendix 9 (V9.12) (All versions < V9.12.10), Mendix Applications using Mendix 9 (V9.18) (All versions < V9.18.4), Mendix Applications using Mendix 9 (V9.6) (All versions < V9.6.15). Some of the Mendix runtime API's allow attackers to bypass	N/A	A-MEN-MEND-270223/772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XPath constraints and retrieve information using XPath queries that trigger errors. **CVE ID : CVE-2023-23835**		
Affected Version(s): From (including) 9.18.0 Up to (excluding) 9.18.4					
Improper Access Control	14-Feb-2023	7.5	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.34), Mendix Applications using Mendix 8 (All versions < V8.18.23), Mendix Applications using Mendix 9 (All versions < V9.22.0), Mendix Applications using Mendix 9 (V9.12) (All versions < V9.12.10), Mendix Applications using Mendix 9 (V9.18) (All versions < V9.18.4), Mendix Applications using Mendix 9 (V9.6) (All versions < V9.6.15). Some of the Mendix runtime API's allow attackers to bypass XPath constraints and retrieve information using XPath queries that trigger errors. **CVE ID : CVE-2023-23835**	N/A	A-MEN-MEND-270223/773
Affected Version(s): From (including) 9.19.0 Up to (excluding) 9.22.0					
Improper Access Control	14-Feb-2023	7.5	A vulnerability has been identified in Mendix Applications using Mendix 7 (All	N/A	A-MEN-MEND-270223/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V7.23.34), Mendix Applications using Mendix 8 (All versions < V8.18.23), Mendix Applications using Mendix 9 (All versions < V9.22.0), Mendix Applications using Mendix 9 (V9.12) (All versions < V9.12.10), Mendix Applications using Mendix 9 (V9.18) (All versions < V9.18.4), Mendix Applications using Mendix 9 (V9.6) (All versions < V9.6.15). Some of the Mendix runtime API's allow attackers to bypass XPath constraints and retrieve information using XPath queries that trigger errors. **CVE ID : CVE-2023-23835**		
Affected Version(s): From (including) 9.7.0 Up to (excluding) 9.12.10					
Improper Access Control	14-Feb-2023	7.5	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.34), Mendix Applications using Mendix 8 (All versions < V8.18.23), Mendix Applications using Mendix 9 (All versions < V9.22.0), Mendix Applications using Mendix 9 (V9.12) (All versions < V9.12.10), Mendix Applications using	N/A	A-MEN-MEND-270223/775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mendix 9 (V9.18) (All versions < V9.18.4), Mendix Applications using Mendix 9 (V9.6) (All versions < V9.6.15). Some of the Mendix runtime API's allow attackers to bypass XPath constraints and retrieve information using XPath queries that trigger errors. **CVE ID : CVE-2023-23835**		
Vendor: Microsoft					
Product: .net					
Affected Version(s): 4.7.1					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	A-MIC-.NET-270223/776
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	A-MIC-.NET-270223/777
Affected Version(s): 2.0					
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	A-MIC-.NET-270223/778
Affected Version(s): 3.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	A-MIC-.NET-270223/779
Affected Version(s): 3.5					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	A-MIC-.NET-270223/780
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	A-MIC-.NET-270223/781
Affected Version(s): 3.5.1					
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	A-MIC-.NET-270223/782
Affected Version(s): 4.6.2					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	A-MIC-.NET-270223/783
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability	https://msrc.microsoft.com/update-	A-MIC-.NET-270223/784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21722	guide/vulnerability/CVE-2023-21722	
Affected Version(s): 4.7					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	A-MIC-.NET-270223/785
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	A-MIC-.NET-270223/786
Affected Version(s): 4.7.2					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	A-MIC-.NET-270223/787
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	A-MIC-.NET-270223/788
Affected Version(s): 4.8					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	A-MIC-.NET-270223/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21808	
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	A-MIC-.NET-270223/790
Affected Version(s): 4.8.1					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	A-MIC-.NET-270223/791
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	A-MIC-.NET-270223/792
Affected Version(s): 6.0.0					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	A-MIC-.NET-270223/793
Affected Version(s): 7.0.0					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	A-MIC-.NET-270223/794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 365_apps					
Affected Version(s): -					
Exposure of Resource to Wrong Sphere	14-Feb-2023	5.5	Microsoft Office Information Disclosure Vulnerability **CVE ID : CVE-2023-21714**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21714	A-MIC-365_-270223/795
Incorrect Authorization	14-Feb-2023	5	Microsoft Publisher Security Features Bypass Vulnerability **CVE ID : CVE-2023-21715**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21715	A-MIC-365_-270223/796
Product: 3d_builder					
Affected Version(s): * Up to (excluding) 20.0.2.0					
N/A	14-Feb-2023	7.8	3D Builder Remote Code Execution Vulnerability **CVE ID : CVE-2023-23377**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23377	A-MIC-3D_B-270223/797
N/A	14-Feb-2023	7.8	3D Builder Remote Code Execution Vulnerability **CVE ID : CVE-2023-23390**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23390	A-MIC-3D_B-270223/798
Product: azure_app_service_on_azure_stack					
Affected Version(s): -					
Improper Privilege Management	14-Feb-2023	8.7	Azure App Service on Azure Stack Hub Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21777**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	A-MIC-AZUR-270223/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21777	
Product: azure_data_box_gateway					
Affected Version(s): -					
N/A	14-Feb-2023	7.2	Azure Data Box Gateway Remote Code Execution Vulnerability **CVE ID : CVE-2023-21703**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21703	A-MIC-AZUR-270223/800
Product: azure_machine_learning					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.02076.0001					
N/A	14-Feb-2023	7.5	Azure Machine Learning Compute Instance Information Disclosure Vulnerability **CVE ID : CVE-2023-23382**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23382	A-MIC-AZUR-270223/801
Product: azure_stack_edge					
Affected Version(s): -					
N/A	14-Feb-2023	7.2	Azure Data Box Gateway Remote Code Execution Vulnerability **CVE ID : CVE-2023-21703**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21703	A-MIC-AZUR-270223/802
Product: defender_for_iot					
Affected Version(s): * Up to (excluding) 22.3.6					
N/A	14-Feb-2023	7.2	Microsoft Defender for IoT Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23379**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23379	A-MIC-DEFE-270223/803
Product: defender_security_intelligence_updates					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.379.200.0					
N/A	14-Feb-2023	7.8	Microsoft Defender for Endpoint Security Feature Bypass Vulnerability **CVE ID : CVE-2023-21809**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21809	A-MIC-DEFE-270223/804
Product: dynamics_365					
Affected Version(s): * Up to (excluding) 4.2.0.51					
N/A	14-Feb-2023	8	Microsoft Dynamics Unified Service Desk Remote Code Execution Vulnerability **CVE ID : CVE-2023-21778**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21778	A-MIC-DYNA-270223/805
Affected Version(s): From (excluding) 9.0 Up to (excluding) 9.0.45.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.5	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-21572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21572	A-MIC-DYNA-270223/806
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.5	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-21807**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21807	A-MIC-DYNA-270223/807
Improper Neutralization of Input During	14-Feb-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	A-MIC-DYNA-270223/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2023-21571**	-2023-21571	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-21573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21573	A-MIC-DYNA-270223/809
Affected Version(s): From (including) 9.0 Up to (excluding) 9.0.45.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-21570**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21570	A-MIC-DYNA-270223/810
Affected Version(s): From (including) 9.1 Up to (excluding) 9.1.16.20					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.5	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-21572**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21572	A-MIC-DYNA-270223/811
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.5	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-21807**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21807	A-MIC-DYNA-270223/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-21570**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21570	A-MIC-DYNA-270223/813
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-21571**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21571	A-MIC-DYNA-270223/814
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-21573**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21573	A-MIC-DYNA-270223/815
Product: edge_chromium					
Affected Version(s): * Up to (excluding) 109.0.15.18.78					
N/A	14-Feb-2023	5.3	Microsoft Edge (Chromium-based) Tampering Vulnerability **CVE ID : CVE-2023-21720**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21720	A-MIC-EDGE-270223/816
Affected Version(s): * Up to (excluding) 110.0.1587.41					
N/A	14-Feb-2023	8.3	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	A-MIC-EDGE-270223/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23374	-2023-23374	
Authentication Bypass by Spoofing	14-Feb-2023	4.3	Microsoft Edge (Chromium-based) Spoofing Vulnerability **CVE ID : CVE-2023-21794**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21794	A-MIC-EDGE-270223/818
Product: exchange_server					
Affected Version(s): 2013					
N/A	14-Feb-2023	8.8	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21529**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21529	A-MIC-EXCH-270223/819
N/A	14-Feb-2023	8.8	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21706**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21706	A-MIC-EXCH-270223/820
N/A	14-Feb-2023	8.8	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21707**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21707	A-MIC-EXCH-270223/821
Affected Version(s): 2016					
N/A	14-Feb-2023	8.8	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21529**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21529	A-MIC-EXCH-270223/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	8.8	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21706**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21706	A-MIC-EXCH-270223/823
N/A	14-Feb-2023	8.8	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21707**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21707	A-MIC-EXCH-270223/824
N/A	14-Feb-2023	7.2	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21710**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21710	A-MIC-EXCH-270223/825
Affected Version(s): 2019					
N/A	14-Feb-2023	8.8	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21529**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21529	A-MIC-EXCH-270223/826
N/A	14-Feb-2023	8.8	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21706**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21706	A-MIC-EXCH-270223/827
N/A	14-Feb-2023	8.8	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21707**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	A-MIC-EXCH-270223/828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21707	
N/A	14-Feb-2023	7.2	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21710**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21710	A-MIC-EXCH-270223/829
Product: office					
Affected Version(s): 2019					
N/A	14-Feb-2023	9.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2023-21716**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716	A-MIC-OFFI-270223/830
Product: office_long_term_servicing_channel					
Affected Version(s): 2021					
N/A	14-Feb-2023	9.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2023-21716**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716	A-MIC-OFFI-270223/831
Exposure of Resource to Wrong Sphere	14-Feb-2023	5.5	Microsoft Office Information Disclosure Vulnerability **CVE ID : CVE-2023-21714**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21714	A-MIC-OFFI-270223/832
Product: office_online_server					
Affected Version(s): 2016					
N/A	14-Feb-2023	9.8	Microsoft Word Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulne	A-MIC-OFFI-270223/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21716	rability/CVE-2023-21716	
Product: office_web_apps					
Affected Version(s): 2013					
N/A	14-Feb-2023	9.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2023-21716**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716	A-MIC-OFFI-270223/834
Product: onenote					
Affected Version(s): * Up to (excluding) 16.0.16026.20158					
N/A	14-Feb-2023	6.5	Microsoft OneNote Spoofing Vulnerability **CVE ID : CVE-2023-21721**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21721	A-MIC-ONEN-270223/835
Product: power_bi_report_server					
Affected Version(s): * Up to (excluding) 15.0.1111.115					
N/A	14-Feb-2023	8.2	Power BI Report Server Spoofing Vulnerability **CVE ID : CVE-2023-21806**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21806	A-MIC-POWE-270223/836
Product: print_3d					
Affected Version(s): * Up to (excluding) 3.3.791					
N/A	14-Feb-2023	7.8	Print 3D Remote Code Execution Vulnerability **CVE ID : CVE-2023-23378**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23378	A-MIC-PRIN-270223/837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sharepoint_enterprise_server					
Affected Version(s): 2013					
N/A	14-Feb-2023	9.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2023-21716**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716	A-MIC-SHAR-270223/838
N/A	14-Feb-2023	8.8	Microsoft SharePoint Server Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21717**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21717	A-MIC-SHAR-270223/839
Affected Version(s): 2016					
N/A	14-Feb-2023	9.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2023-21716**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716	A-MIC-SHAR-270223/840
N/A	14-Feb-2023	8.8	Microsoft SharePoint Server Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21717**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21717	A-MIC-SHAR-270223/841
Product: sharepoint_foundation					
Affected Version(s): 2013					
N/A	14-Feb-2023	9.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2023-21716**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716	A-MIC-SHAR-270223/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	8.8	Microsoft SharePoint Server Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21717**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21717	A-MIC-SHAR-270223/843
Product: sharepoint_server					
Affected Version(s): -					
N/A	14-Feb-2023	9.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2023-21716**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716	A-MIC-SHAR-270223/844
N/A	14-Feb-2023	8.8	Microsoft SharePoint Server Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21717**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21717	A-MIC-SHAR-270223/845
Affected Version(s): 2019					
N/A	14-Feb-2023	9.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2023-21716**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716	A-MIC-SHAR-270223/846
N/A	14-Feb-2023	8.8	Microsoft SharePoint Server Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21717**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21717	A-MIC-SHAR-270223/847
Product: sql_server					
Affected Version(s): 2016					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	8.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21705**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21705	A-MIC-SQL_-270223/848
N/A	14-Feb-2023	8.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21713**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21713	A-MIC-SQL_-270223/849
N/A	14-Feb-2023	7.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21528**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21528	A-MIC-SQL_-270223/850
N/A	14-Feb-2023	7.8	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21704**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21704	A-MIC-SQL_-270223/851
N/A	14-Feb-2023	7.8	Microsoft SQL ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21718**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21718	A-MIC-SQL_-270223/852
Affected Version(s): 2019					
N/A	14-Feb-2023	8.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21705**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	A-MIC-SQL_-270223/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21705	
N/A	14-Feb-2023	8.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21713**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21713	A-MIC-SQL_-270223/854
N/A	14-Feb-2023	7.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21528**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21528	A-MIC-SQL_-270223/855
N/A	14-Feb-2023	7.8	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21704**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21704	A-MIC-SQL_-270223/856
N/A	14-Feb-2023	7.8	Microsoft SQL ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21718**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21718	A-MIC-SQL_-270223/857
Affected Version(s): 2008					
N/A	14-Feb-2023	7.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21528**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21528	A-MIC-SQL_-270223/858
N/A	14-Feb-2023	7.8	Microsoft SQL ODBC Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulne	A-MIC-SQL_-270223/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21718	rability/CVE-2023-21718	
Affected Version(s): 2008_r2					
N/A	14-Feb-2023	7.8	Microsoft SQL ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21718**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21718	A-MIC-SQL_-270223/860
Affected Version(s): 2012					
N/A	14-Feb-2023	8.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21705**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21705	A-MIC-SQL_-270223/861
N/A	14-Feb-2023	8.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21713**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21713	A-MIC-SQL_-270223/862
N/A	14-Feb-2023	7.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21528**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21528	A-MIC-SQL_-270223/863
N/A	14-Feb-2023	7.8	Microsoft SQL ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21718**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21718	A-MIC-SQL_-270223/864
Affected Version(s): 2014					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	8.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21705**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21705	A-MIC-SQL_-270223/865
N/A	14-Feb-2023	8.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21713**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21713	A-MIC-SQL_-270223/866
N/A	14-Feb-2023	7.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21528**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21528	A-MIC-SQL_-270223/867
N/A	14-Feb-2023	7.8	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21704**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21704	A-MIC-SQL_-270223/868
N/A	14-Feb-2023	7.8	Microsoft SQL ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21718**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21718	A-MIC-SQL_-270223/869
Affected Version(s): 2017					
N/A	14-Feb-2023	8.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21705**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	A-MIC-SQL_-270223/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21705	
N/A	14-Feb-2023	8.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21713**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21713	A-MIC-SQL_-270223/871
N/A	14-Feb-2023	7.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21528**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21528	A-MIC-SQL_-270223/872
N/A	14-Feb-2023	7.8	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21704**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21704	A-MIC-SQL_-270223/873
N/A	14-Feb-2023	7.8	Microsoft SQL ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21718**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21718	A-MIC-SQL_-270223/874
Affected Version(s): 2022					
N/A	14-Feb-2023	8.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21705**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21705	A-MIC-SQL_-270223/875
N/A	14-Feb-2023	8.8	Microsoft SQL Server Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulne	A-MIC-SQL_-270223/876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21713	rability/CVE-2023-21713	
N/A	14-Feb-2023	7.8	Microsoft SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21528**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21528	A-MIC-SQL_-270223/877
N/A	14-Feb-2023	7.8	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21704**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21704	A-MIC-SQL_-270223/878
N/A	14-Feb-2023	7.8	Microsoft SQL ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21718**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21718	A-MIC-SQL_-270223/879
Product: sql_server_2019_integration_services					
Affected Version(s): -					
N/A	14-Feb-2023	7.3	Microsoft SQL Server Integration Service (VS extension) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21568**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21568	A-MIC-SQL_-270223/880
Product: sql_server_2022_integration_services					
Affected Version(s): -					
N/A	14-Feb-2023	7.3	Microsoft SQL Server Integration Service (VS extension) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	A-MIC-SQL_-270223/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21568	-2023-21568	
Product: visual_studio_2017					
Affected Version(s): From (including) 15.0 Up to (excluding) 15.9.51					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	A-MIC-VISU-270223/882
Affected Version(s): From (including) 15.0 Up to (excluding) 15.9.52					
N/A	14-Feb-2023	7.8	Visual Studio Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21566**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21566	A-MIC-VISU-270223/883
N/A	14-Feb-2023	7.8	Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21815**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21815	A-MIC-VISU-270223/884
N/A	14-Feb-2023	7.8	Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-23381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23381	A-MIC-VISU-270223/885
N/A	14-Feb-2023	5.6	Visual Studio Denial of Service Vulnerability **CVE ID : CVE-2023-21567**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21567	A-MIC-VISU-270223/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: visual_studio_2019					
Affected Version(s): From (including) 16.0 Up to (excluding) 16.11.24					
N/A	14-Feb-2023	7.8	Visual Studio Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21566**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21566	A-MIC-VISU-270223/887
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	A-MIC-VISU-270223/888
N/A	14-Feb-2023	7.8	Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21815**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21815	A-MIC-VISU-270223/889
N/A	14-Feb-2023	7.8	Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-23381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23381	A-MIC-VISU-270223/890
N/A	14-Feb-2023	5.6	Visual Studio Denial of Service Vulnerability **CVE ID : CVE-2023-21567**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21567	A-MIC-VISU-270223/891
Product: visual_studio_2022					
Affected Version(s): 17.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	A-MIC-VISU-270223/892
Affected Version(s): 17.2					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	A-MIC-VISU-270223/893
Affected Version(s): 17.4					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	A-MIC-VISU-270223/894
Affected Version(s): From (including) 17.0 Up to (excluding) 17.0.19					
N/A	14-Feb-2023	7.8	Visual Studio Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21566**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21566	A-MIC-VISU-270223/895
N/A	14-Feb-2023	7.8	Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21815**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21815	A-MIC-VISU-270223/896
N/A	14-Feb-2023	7.8	Visual Studio Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-	A-MIC-VISU-270223/897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23381	guide/vulnerability/CVE-2023-23381	
N/A	14-Feb-2023	5.6	Visual Studio Denial of Service Vulnerability **CVE ID : CVE-2023-21567**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21567	A-MIC-VISU-270223/898
Affected Version(s): From (including) 17.2 Up to (excluding) 17.2.13					
N/A	14-Feb-2023	7.8	Visual Studio Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21566**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21566	A-MIC-VISU-270223/899
N/A	14-Feb-2023	7.8	Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21815**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21815	A-MIC-VISU-270223/900
N/A	14-Feb-2023	7.8	Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-23381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23381	A-MIC-VISU-270223/901
N/A	14-Feb-2023	5.6	Visual Studio Denial of Service Vulnerability **CVE ID : CVE-2023-21567**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21567	A-MIC-VISU-270223/902
Affected Version(s): From (including) 17.4 Up to (excluding) 17.4.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.8	Visual Studio Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21566**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21566	A-MIC-VISU-270223/903
N/A	14-Feb-2023	7.8	Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21815**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21815	A-MIC-VISU-270223/904
N/A	14-Feb-2023	7.8	Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-23381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23381	A-MIC-VISU-270223/905
N/A	14-Feb-2023	5.6	Visual Studio Denial of Service Vulnerability **CVE ID : CVE-2023-21567**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21567	A-MIC-VISU-270223/906
Product: word					
Affected Version(s): 2013					
N/A	14-Feb-2023	9.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2023-21716**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716	A-MIC-WORD-270223/907
Vendor: Microweber					
Product: microweber					
Affected Version(s): * Up to (excluding) 1.3.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Feb-2023	5.4	Cross-site Scripting (XSS) - DOM in GitHub repository microweber/microweber prior to 1.3.2. **CVE ID : CVE-2023-0608**	https://github.com/microweber/microweber/commit/20df56615e61624f5fff149849753869e4b3b936, https://huntr.dev/bounties/02a86e0d-dff7-4e27-89d5-2f7dcd4b580c	A-MIC-MICR-270223/908
Vendor: Mitel					
Product: micontact_center_business					
Affected Version(s): From (including) 9.2.2.0 Up to (excluding) 9.4.2.0					
N/A	13-Feb-2023	7.5	The ccmweb component of Mitel MiContact Center Business server 9.2.2.0 through 9.4.1.0 could allow an unauthenticated attacker to download arbitrary files, due to insufficient restriction of URL parameters. A successful exploit could allow access to sensitive information. **CVE ID : CVE-2023-22854**	https://www.mitel.com/support/security-advisories, https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-23-0001	A-MIT-MICO-270223/909
Vendor: modoboa					
Product: modoboa					
Affected Version(s): * Up to (excluding) 2.0.4					
N/A	10-Feb-2023	9.8	Authentication Bypass by Primary Weakness in GitHub repository	https://github.com/modoboa/modob	A-MOD-MODO-270223/910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modoboa/modoboa prior to 2.0.4. **CVE ID : CVE-2023-0777**	oa/commit/47d17ac6643f870719691073956a26e4be0a4806, https://huntr.dev/bounties/a17e7a9f-0fee-4130-a522-5a0466fc17c7	
Vendor: mojojson_project					
Product: mojojson					
Affected Version(s): 1.2.3					
Out-of-bounds Write	03-Feb-2023	9.8	Buffer OverFlow Vulnerability in MojoJson v1.2.3 allows an attacker to execute arbitrary code via the SkipString function. **CVE ID : CVE-2023-23086**	N/A	A-MOJ-MOJO-270223/911
NULL Pointer Dereference	03-Feb-2023	9.8	An issue was found in MojoJson v1.2.3 allows attackers to execute arbitary code via the destroy function. **CVE ID : CVE-2023-23087**	N/A	A-MOJ-MOJO-270223/912
Vendor: mojoportal					
Product: mojoportal					
Affected Version(s): 2.7.0.0					
Improper Restriction of XML External Entity Reference	09-Feb-2023	8.8	Mojoportal v2.7 was discovered to contain an authenticated XML external entity (XXE) injection vulnerability. **CVE ID : CVE-2023-24323**	N/A	A-MOJ-MOJO-270223/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Feb-2023	6.1	A reflected cross-site scripting (XSS) vulnerability in the FileDialog.aspx component of mojoPortal v2.7.0.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the ed and tbi parameters. **CVE ID : CVE-2023-24322**	N/A	A-MOJ-MOJO-270223/914
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Feb-2023	5.4	Mojoportal v2.7.0.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the Company Info Settings component. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the txtCompanyName parameter. **CVE ID : CVE-2023-24687**	N/A	A-MOJ-MOJO-270223/915
N/A	09-Feb-2023	5.3	An issue in Mojoportal v2.7.0.0 allows an unauthenticated attacker to register a new user even if the Allow User Registrations feature is disabled. **CVE ID : CVE-2023-24688**	N/A	A-MOJ-MOJO-270223/916
Improper Limitation	09-Feb-2023	4.3	An issue in Mojoportal v2.7.0.0 and below	N/A	A-MOJ-MOJO-270223/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			allows an authenticated attacker to list all css files inside the root path of the webserver via manipulation of the "s" parameter in /DesignTools/ManageSkin.aspx **CVE ID : CVE-2023-24689**		
Vendor: monsterinsights					
Product: monsterinsights					
Affected Version(s): * Up to (excluding) 8.12.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The MonsterInsights WordPress plugin before 8.12.1 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0081**	N/A	A-MON-MONS-270223/918
Vendor: naver_map_project					
Product: naver_map					
Affected Version(s): * Up to (including) 1.1.0					
Improper Neutralization of Input During Web Page Generation	06-Feb-2023	5.4	The Naver Map WordPress plugin through 1.1.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed,	N/A	A-NAV-NAVE-270223/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0146**		
Vendor: NEC					
Product: pc_settings_tool					
Affected Version(s): From (including) 10.0.0.0 Up to (including) 10.1.26.0					
N/A	15-Feb-2023	7.8	PC settings tool Ver10.1.26.0 and earlier, PC settings tool Ver11.0.22.0 and earlier allows a attacker to write to the registry as administrator privileges with standard user privileges. **CVE ID : CVE-2023-25011**	N/A	A-NEC-PC_S-270223/920
Affected Version(s): From (including) 11.0.0.0 Up to (including) 11.0.22.0					
N/A	15-Feb-2023	7.8	PC settings tool Ver10.1.26.0 and earlier, PC settings tool Ver11.0.22.0 and earlier allows a attacker to write to the registry as administrator privileges with standard user privileges. **CVE ID : CVE-2023-25011**	N/A	A-NEC-PC_S-270223/921
Vendor: Nextcloud					
Product: desktop					
Affected Version(s): * Up to (excluding) 3.6.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	6.1	The Nextcloud Desktop Client is a tool to synchronize files from a Nextcloud Server with your computer. Versions prior to 3.6.3 are missing sanitisation on qml labels which are used for basic HTML elements such as `strong`, `em` and `head` lines in the UI of the desktop client. The lack of sanitisation may allow for javascript injection. It is recommended that the Nextcloud Desktop Client is upgraded to 3.6.3. There are no known workarounds for this issue. **CVE ID : CVE-2023-23942**	https://github.com/nextcloud/desktop/pull/5233, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-64qc-vf6v-8xgg	A-NEX-DESK-270223/922
Product: mail					
Affected Version(s): * Up to (excluding) 1.11.8					
Authorization Bypass Through User-Controlled Key	13-Feb-2023	5.3	Nextcloud Mail is an email app for the Nextcloud home server platform. Prior to versions 2.2.1, 1.14.5, 1.12.9, and 1.11.8, an attacker can access the mail box by ID getting the subjects and the first characters of the emails. Users should upgrade to Mail 2.2.1 for Nextcloud 25, Mail 1.14.5 for Nextcloud 22-24, Mail 1.12.9 for Nextcloud 21, or Mail 1.11.8 for Nextcloud 20	https://github.com/nextcloud/mail/pull/7740, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-m45f-r5gh-h6cx	A-NEX-MAIL-270223/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to receive a patch. No known workarounds are available. **CVE ID : CVE-2023-25160**		
Affected Version(s): * Up to (excluding) 1.15.0					
Server-Side Request Forgery (SSRF)	06-Feb-2023	4.3	Nextcloud mail is an email app for the nextcloud home server platform. In affected versions the SMTP, IMAP and Sieve host fields allowed to scan for internal services and servers reachable from within the local network of the Nextcloud Server. It is recommended that the Nextcloud Maill app is upgraded to 1.15.0 or 2.2.2. The only known workaround for this issue is to completely disable the nextcloud mail app. **CVE ID : CVE-2023-23943**	https://github.com/nextcloud/mail/pull/7796, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8gcx-r739-9pf6	A-NEX-MAIL-270223/924
Affected Version(s): * Up to (excluding) 2.2.2					
Cleartext Storage of Sensitive Information	06-Feb-2023	6.5	Nextcloud mail is an email app for the nextcloud home server platform. In versions prior to 2.2.2 user's passwords were stored in cleartext in the database during the duration of OAuth2 setup procedure. Any attacker or malicious user with access to the database would have	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-g86r-x755-93f4, https://github.com/nextcloud/mail/pull/7797	A-NEX-MAIL-270223/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to these user passwords until the OAuth setup has been completed. It is recommended that the Nextcloud Mail app is upgraded to 2.2.2. There are no known workarounds for this issue. **CVE ID : CVE-2023-23944**		
Affected Version(s): From (including) 1.12.0 Up to (excluding) 1.12.9					
Authorization Bypass Through User-Controlled Key	13-Feb-2023	5.3	Nextcloud Mail is an email app for the Nextcloud home server platform. Prior to versions 2.2.1, 1.14.5, 1.12.9, and 1.11.8, an attacker can access the mail box by ID getting the subjects and the first characters of the emails. Users should upgrade to Mail 2.2.1 for Nextcloud 25, Mail 1.14.5 for Nextcloud 22-24, Mail 1.12.9 for Nextcloud 21, or Mail 1.11.8 for Nextcloud 20 to receive a patch. No known workarounds are available. **CVE ID : CVE-2023-25160**	https://github.com/nextcloud/mail/pull/7740, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-m45f-r5gh-h6cx	A-NEX-MAIL-270223/926
Affected Version(s): From (including) 1.13.0 Up to (excluding) 1.14.5					
Authorization Bypass Through User-Controlled Key	13-Feb-2023	5.3	Nextcloud Mail is an email app for the Nextcloud home server platform. Prior to versions 2.2.1, 1.14.5, 1.12.9, and 1.11.8, an	https://github.com/nextcloud/mail/pull/7740, https://github.com/next	A-NEX-MAIL-270223/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can access the mail box by ID getting the subjects and the first characters of the emails. Users should upgrade to Mail 2.2.1 for Nextcloud 25, Mail 1.14.5 for Nextcloud 22-24, Mail 1.12.9 for Nextcloud 21, or Mail 1.11.8 for Nextcloud 20 to receive a patch. No known workarounds are available. **CVE ID : CVE-2023-25160**	cloud/security-advisories/security/advisories/GHSA-m45f-r5gh-h6cx	
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.2.1					
Authorization Bypass Through User-Controlled Key	13-Feb-2023	5.3	Nextcloud Mail is an email app for the Nextcloud home server platform. Prior to versions 2.2.1, 1.14.5, 1.12.9, and 1.11.8, an attacker can access the mail box by ID getting the subjects and the first characters of the emails. Users should upgrade to Mail 2.2.1 for Nextcloud 25, Mail 1.14.5 for Nextcloud 22-24, Mail 1.12.9 for Nextcloud 21, or Mail 1.11.8 for Nextcloud 20 to receive a patch. No known workarounds are available. **CVE ID : CVE-2023-25160**	https://github.com/nextcloud/mail/pull/7740, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-m45f-r5gh-h6cx	A-NEX-MAIL-270223/928
Affected Version(s): From (including) 2.2.0 Up to (excluding) 2.2.2					
Server-Side	06-Feb-2023	4.3	Nextcloud mail is an email app for the	https://github.com/next	A-NEX-MAIL-270223/929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (SSRF)			nextcloud home server platform. In affected versions the SMTP, IMAP and Sieve host fields allowed to scan for internal services and servers reachable from within the local network of the Nextcloud Server. It is recommended that the Nextcloud Maill app is upgraded to 1.15.0 or 2.2.2. The only known workaround for this issue is to completely disable the nextcloud mail app. **CVE ID : CVE-2023-23943**	cloud/mail/pull/7796, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8gcx-r739-9pf6	
Product: nextcloud_server					
Affected Version(s): * Up to (excluding) 23.0.12					
N/A	13-Feb-2023	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 25.0.1 24.0.8, and 23.0.12 missing rate limiting on password reset functionality. This could result in service slowdown, storage overflow, or cost impact when using external email services. Users should upgrade to Nextcloud Server 25.0.1, 24.0.8, or 23.0.12 or Nextcloud Enterprise Server	https://github.com/nextcloud/server/pull/34632, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-492h-596q-xr2f	A-NEX-NEXT-270223/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			25.0.1, 24.0.8, or 23.0.12 to receive a patch. No known workarounds are available. **CVE ID : CVE-2023-25161**		
Server-Side Request Forgery (SSRF)	13-Feb-2023	5.3	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. Nextcloud Server prior to 24.0.8 and 23.0.12 and Nextcloud Enterprise server prior to 24.0.8 and 23.0.12 are vulnerable to server-side request forgery (SSRF). Attackers can leverage enclosed alphanumeric payloads to bypass IP filters and gain SSRF, which would allow an attacker to read crucial metadata if the server is hosted on the AWS platform. Nextcloud Server 24.0.8 and 23.0.2 and Nextcloud Enterprise Server 24.0.8 and 23.0.12 contain a patch for this issue. No known workarounds are available. **CVE ID : CVE-2023-25162**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-mqrx-grp7-244m	A-NEX-NEXT-270223/931
Affected Version(s): 24.0.2					
N/A	13-Feb-2023	5.3	Nextcloud Server is the file server software for Nextcloud, a self-hosted	https://github.com/nextcloud/securi	A-NEX-NEXT-270223/932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			productivity platform, and Nextcloud Office is a document collaboration app for the same platform. Nextcloud Server 24.0.x prior to 24.0.8 and 25.0.x prior to 25.0.1, Nextcloud Enterprise Server 24.0.x prior to 24.0.8 and 25.0.x prior to 25.0.1, and Nextcloud Office (Richdocuments) App 6.x prior to 6.3.1 and 7.x prior to 7.0.1 have previews accessible without a watermark. The download should be hidden and the watermark should get applied. This issue is fixed in Nextcloud Server 25.0.1 and 24.0.8, Nextcloud Enterprise Server 25.0.1 and 24.0.8, and Nextcloud Office (Richdocuments) App 7.0.1 (for 25) and 6.3.1 (for 24). No known workarounds are available. **CVE ID : CVE-2023-25159**	ty-advisories/security/advisories/GHSA-92g2-h5jv-jjmg	
Affected Version(s): 25.0.0					
N/A	13-Feb-2023	5.3	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Office is a document collaboration app for	https://github.com/nextcloud/security-advisories/security/advisories/GHSA	A-NEX-NEXT-270223/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the same platform. Nextcloud Server 24.0.x prior to 24.0.8 and 25.0.x prior to 25.0.1, Nextcloud Enterprise Server 24.0.x prior to 24.0.8 and 25.0.x prior to 25.0.1, and Nextcloud Office (Richdocuments) App 6.x prior to 6.3.1 and 7.x prior to 7.0.1 have previews accessible without a watermark. The download should be hidden and the watermark should get applied. This issue is fixed in Nextcloud Server 25.0.1 and 24.0.8, Nextcloud Enterprise Server 25.0.1 and 24.0.8, and Nextcloud Office (Richdocuments) App 7.0.1 (for 25) and 6.3.1 (for 24). No known workarounds are available. **CVE ID : CVE-2023-25159**	-92g2-h5jv-jjmg	
N/A	13-Feb-2023	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 25.0.1 24.0.8, and 23.0.12 missing rate limiting on password reset functionality. This could result in service	https://github.com/nextcloud/server/pull/34632, https://github.com/nextcloud/security-advisories/security/advisories/GHSA	A-NEX-NEXT-270223/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			slowdown, storage overflow, or cost impact when using external email services. Users should upgrade to Nextcloud Server 25.0.1, 24.0.8, or 23.0.12 or Nextcloud Enterprise Server 25.0.1, 24.0.8, or 23.0.12 to receive a patch. No known workarounds are available. **CVE ID : CVE-2023-25161**	-492h-596q-xr2f	
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.8					
N/A	13-Feb-2023	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 25.0.1 24.0.8, and 23.0.12 missing rate limiting on password reset functionality. This could result in service slowdown, storage overflow, or cost impact when using external email services. Users should upgrade to Nextcloud Server 25.0.1, 24.0.8, or 23.0.12 or Nextcloud Enterprise Server 25.0.1, 24.0.8, or 23.0.12 to receive a patch. No known workarounds are available.	https://github.com/nextcloud/server/pull/34632, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-492h-596q-xr2f	A-NEX-NEXT-270223/935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25161		
Server-Side Request Forgery (SSRF)	13-Feb-2023	5.3	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. Nextcloud Server prior to 24.0.8 and 23.0.12 and Nextcloud Enterprise server prior to 24.0.8 and 23.0.12 are vulnerable to server-side request forgery (SSRF). Attackers can leverage enclosed alphanumeric payloads to bypass IP filters and gain SSRF, which would allow an attacker to read crucial metadata if the server is hosted on the AWS platform. Nextcloud Server 24.0.8 and 23.0.2 and Nextcloud Enterprise Server 24.0.8 and 23.0.12 contain a patch for this issue. No known workarounds are available. **CVE ID : CVE-2023-25162**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-mqrx-grp7-244m	A-NEX-NEXT-270223/936
Affected Version(s): From (including) 24.0.4 Up to (including) 24.0.8					
N/A	13-Feb-2023	5.3	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Office is a document collaboration app for the same platform. Nextcloud Server 24.0.x	https://github.com/nextcloud/security-advisories/security/advisories/GHSA	A-NEX-NEXT-270223/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 24.0.8 and 25.0.x prior to 25.0.1, Nextcloud Enterprise Server 24.0.x prior to 24.0.8 and 25.0.x prior to 25.0.1, and Nextcloud Office (Richdocuments) App 6.x prior to 6.3.1 and 7.x prior to 7.0.1 have previews accessible without a watermark. The download should be hidden and the watermark should get applied. This issue is fixed in Nextcloud Server 25.0.1 and 24.0.8, Nextcloud Enterprise Server 25.0.1 and 24.0.8, and Nextcloud Office (Richdocuments) App 7.0.1 (for 25) and 6.3.1 (for 24). No known workarounds are available. **CVE ID : CVE-2023-25159**	-92g2-h5jv-jjmg	
Product: richdocuments					
Affected Version(s): 7.0.0					
N/A	13-Feb-2023	5.3	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Office is a document collaboration app for the same platform. Nextcloud Server 24.0.x prior to 24.0.8 and 25.0.x prior to 25.0.1, Nextcloud Enterprise	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-92g2-h5jv-jjmg	A-NEX-RICH-270223/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server 24.0.x prior to 24.0.8 and 25.0.x prior to 25.0.1, and Nextcloud Office (Richdocuments) App 6.x prior to 6.3.1 and 7.x prior to 7.0.1 have previews accessible without a watermark. The download should be hidden and the watermark should get applied. This issue is fixed in Nextcloud Server 25.0.1 and 24.0.8, Nextcloud Enterprise Server 25.0.1 and 24.0.8, and Nextcloud Office (Richdocuments) App 7.0.1 (for 25) and 6.3.1 (for 24). No known workarounds are available. **CVE ID : CVE-2023-25159**		
Affected Version(s): * Up to (excluding) 3.8.7					
Incorrect Permission Assignment for Critical Resource	08-Feb-2023	5.7	Nextcloud office/richdocuments is an office suit for the nextcloud server platform. In affected versions the Collabora integration can be tricked to provide access to any file without proper permission validation. As a result any user with access to Collabora can obtain the content of other users files. It is recommended that the	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-64xc-r58v-53gj, https://github.com/nextcloud/richdocuments/pull/2669	A-NEX-RICH-270223/939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Nextcloud Office App (Collabora Integration) is updated to 7.0.2 (Nextcloud 25), 6.3.2 (Nextcloud 24), 5.0.10 (Nextcloud 23), 4.2.9 (Nextcloud 21-22), or 3.8.7 (Nextcloud 15-20). There are no known workarounds for this issue. **CVE ID : CVE-2023-25150**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.9					
Incorrect Permission Assignment for Critical Resource	08-Feb-2023	5.7	Nextcloud office/richdocuments is an office suit for the nextcloud server platform. In affected versions the Collabora integration can be tricked to provide access to any file without proper permission validation. As a result any user with access to Collabora can obtain the content of other users files. It is recommended that the Nextcloud Office App (Collabora Integration) is updated to 7.0.2 (Nextcloud 25), 6.3.2 (Nextcloud 24), 5.0.10 (Nextcloud 23), 4.2.9 (Nextcloud 21-22), or 3.8.7 (Nextcloud 15-20). There are no known workarounds for this issue.	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-64xc-r58v-53gj, https://github.com/nextcloud/richdocuments/pull/2669	A-NEX-RICH-270223/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25150		
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.0.10					
Incorrect Permission Assignment for Critical Resource	08-Feb-2023	5.7	Nextcloud office/richdocuments is an office suit for the nextcloud server platform. In affected versions the Collabora integration can be tricked to provide access to any file without proper permission validation. As a result any user with access to Collabora can obtain the content of other users files. It is recommended that the Nextcloud Office App (Collabora Integration) is updated to 7.0.2 (Nextcloud 25), 6.3.2 (Nextcloud 24), 5.0.10 (Nextcloud 23), 4.2.9 (Nextcloud 21-22), or 3.8.7 (Nextcloud 15-20). There are no known workarounds for this issue. **CVE ID : CVE-2023-25150**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-64xc-r58v-53gj, https://github.com/nextcloud/richdocuments/pull/2669	A-NEX-RICH-270223/941
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.3.1					
N/A	13-Feb-2023	5.3	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Office is a document collaboration app for the same platform. Nextcloud Server 24.0.x	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-92g2-h5jv-jjmg	A-NEX-RICH-270223/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 24.0.8 and 25.0.x prior to 25.0.1, Nextcloud Enterprise Server 24.0.x prior to 24.0.8 and 25.0.x prior to 25.0.1, and Nextcloud Office (Richdocuments) App 6.x prior to 6.3.1 and 7.x prior to 7.0.1 have previews accessible without a watermark. The download should be hidden and the watermark should get applied. This issue is fixed in Nextcloud Server 25.0.1 and 24.0.8, Nextcloud Enterprise Server 25.0.1 and 24.0.8, and Nextcloud Office (Richdocuments) App 7.0.1 (for 25) and 6.3.1 (for 24). No known workarounds are available. **CVE ID : CVE-2023-25159**		
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.3.2					
Incorrect Permission Assignment for Critical Resource	08-Feb-2023	5.7	Nextcloud office/richdocuments is an office suit for the nextcloud server platform. In affected versions the Collabora integration can be tricked to provide access to any file without proper permission validation. As a result any user with access to Collabora	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-64xc-r58v-53gj, https://github.com/nextcloud/richd	A-NEX-RICH-270223/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can obtain the content of other users files. It is recommended that the Nextcloud Office App (Collabora Integration) is updated to 7.0.2 (Nextcloud 25), 6.3.2 (Nextcloud 24), 5.0.10 (Nextcloud 23), 4.2.9 (Nextcloud 21-22), or 3.8.7 (Nextcloud 15-20). There are no known workarounds for this issue. **CVE ID : CVE-2023-25150**	ocuments/pull/2669	
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.2					
Incorrect Permission Assignment for Critical Resource	08-Feb-2023	5.7	Nextcloud office/richdocuments is an office suit for the nextcloud server platform. In affected versions the Collabora integration can be tricked to provide access to any file without proper permission validation. As a result any user with access to Collabora can obtain the content of other users files. It is recommended that the Nextcloud Office App (Collabora Integration) is updated to 7.0.2 (Nextcloud 25), 6.3.2 (Nextcloud 24), 5.0.10 (Nextcloud 23), 4.2.9 (Nextcloud 21-22), or 3.8.7 (Nextcloud 15-20). There are no	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-64xc-r58v-53gj, https://github.com/nextcloud/richdocuments/pull/2669	A-NEX-RICH-270223/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workarounds for this issue. **CVE ID : CVE-2023-25150**		
Vendor: nosh_chartingsystem_project					
Product: nosh_chartingsystem					
Affected Version(s): 2021-03-13					
Unrestricted Upload of File with Dangerous Type	01-Feb-2023	8.8	NOSH 4a5cfdb allows remote authenticated users to execute PHP arbitrary code via the "practice logo" upload feature. The client-side checks can be bypassed. This may allow attackers to steal Protected Health Information because the product is for health charting. **CVE ID : CVE-2023-24610**	N/A	A-NOS-NOSH-270223/945
Vendor: objectcomputing					
Product: opendds					
Affected Version(s): * Up to (excluding) 3.23.1					
N/A	03-Feb-2023	7.5	OpenDDS is an open source C++ implementation of the Object Management Group (OMG) Data Distribution Service (DDS). OpenDDS applications that are exposed to untrusted RTPS network traffic may crash when parsing badly-formed input. This issue has been patched in version 3.23.1.	https://github.com/OpenDDS/OpenDDS/security/advisories/GHSA-8wvq-25f5-f8h4	A-OBJ-OPEN-270223/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23932		
Vendor: okfn					
Product: ckan					
Affected Version(s): * Up to (excluding) 2.8.12					
Use of Insufficiently Random Values	03-Feb-2023	7.5	CKAN is an open-source DMS (data management system) for powering data hubs and data portals. When creating a new container based on one of the Docker images listed below, the same secret key was being used by default. If the users didn't set a custom value via environment variables in the `.env` file, that key was shared across different CKAN instances, making it easy to forge authentication requests. Users overriding the default secret key in their own `.env` file are not affected by this issue. Note that the legacy images (ckan/ckan) located in the main CKAN repo are not affected by this issue. The affected images are ckan/ckan-docker, (ckan/ckan-base images), okfn/docker-ckan (openknowledge/ckan-base and openknowledge/ckan-dev images)	https://github.com/ckan/ckan/commit/4c22c135fa486afa13855d1cdb9765eaf418d2aa, https://github.com/ckan/ckan/commit/44af0f0a148fcc0e0fbcf02fe69b7db13459a84b	A-OKF-CKAN-270223/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			keitaroinc/docker-ckan (keitaro/ckan images). **CVE ID : CVE-2023-22746**		
Affected Version(s): From (including) 2.9.0 Up to (excluding) 2.9.7					
Use of Insufficiently Random Values	03-Feb-2023	7.5	CKAN is an open-source DMS (data management system) for powering data hubs and data portals. When creating a new container based on one of the Docker images listed below, the same secret key was being used by default. If the users didn't set a custom value via environment variables in the `.env` file, that key was shared across different CKAN instances, making it easy to forge authentication requests. Users overriding the default secret key in their own `.env` file are not affected by this issue. Note that the legacy images (ckan/ckan) located in the main CKAN repo are not affected by this issue. The affected images are ckan/ckan-docker, (ckan/ckan-base images), okfn/docker-ckan (openknowledge/ckan-base and openknowledge/ckan-dev images)	https://github.com/ckan/ckan/commit/4c22c135fa486afa13855d1cdb9765eaf418d2aa, https://github.com/ckan/ckan/commit/44af0f0a148fcc0e0fbcf02fe69b7db13459a84b	A-OKF-CKAN-270223/948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			keitaroinc/docker-ckan (keitaro/ckan images). **CVE ID : CVE-2023-22746**		
Vendor: onedev_project					
Product: onedev					
Affected Version(s): * Up to (excluding) 7.9.12					
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	08-Feb-2023	8.8	Onedev is a self-hosted Git Server with CI/CD and Kanban. In versions prior to 7.9.12 the algorithm used to generate access token and password reset keys was not cryptographically secure. Existing normal users (or everyone if it allows self-registration) may exploit this to elevate privilege to obtain administrator permission. This issue is has been addressed in version 7.9.12. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-24828**	https://github.com/theonedev/onedev/commit/d67dd9686897fe5e4ab881d749464aa7c06a68e5	A-ONE-ONED-270223/949
Vendor: online_eyewear_shop_project					
Product: online_eyewear_shop					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL	04-Feb-2023	9.8	A vulnerability classified as critical was found in SourceCodester Online Eyewear Shop 1.0. Affected by this vulnerability is an	N/A	A-ONL-ONLI-270223/950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			unknown functionality of the file oews/?p=products/view_product.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-220195. **CVE ID : CVE-2023-0673**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Feb-2023	9.8	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been classified as critical. This affects the function update_cart of the file /oews/classes/Master.php?f=update_cart of the component HTTP POST Request Handler. The manipulation of the argument cart_id leads to sql injection. It is possible to initiate the attack remotely. The identifier VDB-220245 was assigned to this vulnerability. **CVE ID : CVE-2023-0686**	N/A	A-ONL-ONLI-270223/951
Improper Neutralization of Input During Web Page Generation	07-Feb-2023	6.1	A vulnerability has been found in SourceCodester Online Eyewear Shop 1.0 and classified as problematic. Affected by this vulnerability is	N/A	A-ONL-ONLI-270223/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			the function registration of the file oews/classes/Users.php of the component POST Request Handler. The manipulation of the argument firstname/middlename/lastname/email/contact leads to cross site scripting. The attack can be launched remotely. The identifier VDB-220369 was assigned to this vulnerability. **CVE ID : CVE-2023-0732**		
Vendor: online_food_ordering_system_project					
Product: online_food_ordering_system					
Affected Version(s): 2.0					
Unrestricted Upload of File with Dangerous Type	13-Feb-2023	9.8	An arbitrary file upload vulnerability in the component /fos/admin/ajax.php of Food Ordering System v2.0 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2023-24646**	N/A	A-ONL-ONLI-270223/953
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Feb-2023	7.5	Food Ordering System v2.0 was discovered to contain a SQL injection vulnerability via the email parameter. **CVE ID : CVE-2023-24647**	N/A	A-ONL-ONLI-270223/954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	6.1	Online Food Ordering System v2 was discovered to contain a cross-site scripting (XSS) vulnerability via the redirect parameter in signup.php. **CVE ID : CVE-2023-24191**	N/A	A-ONL-ONLI-270223/955
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	6.1	Online Food Ordering System v2 was discovered to contain a cross-site scripting (XSS) vulnerability via the redirect parameter in login.php. **CVE ID : CVE-2023-24192**	N/A	A-ONL-ONLI-270223/956
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	6.1	Online Food Ordering System v2 was discovered to contain a cross-site scripting (XSS) vulnerability via the page parameter in navbar.php. **CVE ID : CVE-2023-24194**	N/A	A-ONL-ONLI-270223/957
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	6.1	Online Food Ordering System v2 was discovered to contain a cross-site scripting (XSS) vulnerability via the page parameter in index.php. **CVE ID : CVE-2023-24195**	N/A	A-ONL-ONLI-270223/958
Improper Neutralization of Input During	06-Feb-2023	6.1	Online Food Ordering System v2 was discovered to contain a SQL injection vulnerability via the id	N/A	A-ONL-ONLI-270223/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			parameter at view_order.php. **CVE ID : CVE-2023-24197**		
Vendor: open5gs					
Product: open5gs					
Affected Version(s): * Up to (excluding) 2.4.13					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	Due to insufficient length validation in the Open5GS GTP library versions prior to versions 2.4.13 and 2.5.7, when parsing extension headers in GPRS tunneling protocol (GPTv1-U) messages, a protocol payload with any extension header length set to zero causes an infinite loop. The affected process becomes immediately unresponsive, resulting in denial of service and excessive resource consumption. CVSS3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C **CVE ID : CVE-2023-23846**	N/A	A-OPE-OPEN-270223/960
Affected Version(s): 2.5.6					
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	Due to insufficient length validation in the Open5GS GTP library versions prior to versions 2.4.13 and 2.5.7, when parsing extension headers in GPRS tunneling	N/A	A-OPE-OPEN-270223/961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocol (GPTv1-U) messages, a protocol payload with any extension header length set to zero causes an infinite loop. The affected process becomes immediately unresponsive, resulting in denial of service and excessive resource consumption. CVSS3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C **CVE ID : CVE-2023-23846**		
Vendor: Openssh					
Product: openssh					
Affected Version(s): 9.1					
Double Free	03-Feb-2023	9.8	OpenSSH server (sshd) 9.1 introduced a double-free vulnerability during options.kex_algorithms handling. This is fixed in OpenSSH 9.2. The double free can be leveraged, by an unauthenticated remote attacker in the default configuration, to jump to any location in the sshd address space. One third-party report states "remote code execution is theoretically possible." **CVE ID : CVE-2023-25136**	https://ftp.openbsd.org/pub/OpenBSD/patches/7.2/common/017_sshd.patch.sig, https://github.com/openssh/openssh-portable/commit/486c4dc3b83b4b67d663fb0fa62bc24138ec3946	A-OPE-OPEN-270223/962
Vendor: Openssl					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: openssl					
Affected Version(s): From (including) 1.0.2 Up to (excluding) 1.0.2zg					
Use After Free	08-Feb-2023	7.5	The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. The function receives a BIO from the caller, prepends a new BIO_f_asn1 filter BIO onto the front of it to form a BIO chain, and then returns the new head of the BIO chain to the caller. Under certain conditions, for example if a CMS recipient public key is invalid, the new filter BIO is freed and the function returns a NULL result indicating a failure. However, in this case, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to the previously freed filter BIO. If the caller then goes on to call BIO_pop() on the BIO then a use-after-free will occur. This will most likely result in a crash. This scenario	https://www.openssl.org/news/secadv/20230207.txt	A-OPE-OPEN-270223/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occurs directly in the internal function B64_write_ASN1() which may cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() on the BIO. This internal function is in turn called by the public API functions PEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream, SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7. Other public API functions that may be impacted by this include i2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream and i2d_PKCS7_bio_stream. The OpenSSL cms and smime command line applications are similarly affected. **CVE ID : CVE-2023-0215**		
Access of Resource Using Incompatible Type ('Type Confusion')	08-Feb-2023	7.4	There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed	https://www.openssl.org/news/secadv/20230207.txt	A-OPE-OPEN-270223/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have implemented their own functionality for retrieving CRLs over a network. **CVE ID : CVE-2023-0286**		
Affected Version(s): From (including) 1.1.1 Up to (excluding) 1.1.1t					
Use After Free	08-Feb-2023	7.5	The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. The function receives a BIO from the caller, prepends a new BIO_f_asn1 filter BIO onto the front of it to form a BIO chain, and then returns the new head of the BIO chain to the caller. Under certain conditions, for example if a CMS recipient public key is invalid, the new filter BIO is freed and the function returns a NULL result indicating a failure. However, in this case, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to the previously freed filter BIO. If the caller then	https://www.openssl.org/news/secadv/20230207.txt	A-OPE-OPEN-270223/965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			goes on to call BIO_pop() on the BIO then a use-after-free will occur. This will most likely result in a crash. This scenario occurs directly in the internal function B64_write_ASN1() which may cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() on the BIO. This internal function is in turn called by the public API functions PEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream, SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7. Other public API functions that may be impacted by this include i2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream and i2d_PKCS7_bio_stream. The OpenSSL cms and smime command line applications are similarly affected. **CVE ID : CVE-2023-0215**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	08-Feb-2023	7.4	There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must	https://www.openssl.org/news/secadv/20230207.txt	A-OPE-OPEN-270223/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network. **CVE ID : CVE-2023-0286**		
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.8					
Use After Free	08-Feb-2023	7.5	The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. The function receives a BIO from the caller, prepends a new BIO_f_asn1 filter BIO onto the front of it to form a BIO chain, and then returns the new head of the BIO chain to the caller. Under certain conditions, for example if a CMS recipient public key is invalid, the new filter BIO is freed and the function returns a NULL result indicating a failure. However, in this	https://www.openssl.org/news/secadv/20230207.txt	A-OPE-OPEN-270223/967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			case, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to the previously freed filter BIO. If the caller then goes on to call BIO_pop() on the BIO then a use-after-free will occur. This will most likely result in a crash. This scenario occurs directly in the internal function B64_write_ASN1() which may cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() on the BIO. This internal function is in turn called by the public API functions PEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream, SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7. Other public API functions that may be impacted by this include i2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream and i2d_PKCS7_bio_stream. The OpenSSL cms and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			smime command line applications are similarly affected. **CVE ID : CVE-2023-0215**		
Access of Resource Using Incompatible Type ('Type Confusion')	08-Feb-2023	7.4	There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and	https://www.openssl.org/news/secadv/20230207.txt	A-OPE-OPEN-270223/968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network. **CVE ID : CVE-2023-0286**		
Affected Version(s): From (including) 3.0.0 Up to (including) 3.0.7					
NULL Pointer Dereference	08-Feb-2023	7.5	An invalid pointer dereference on read can be triggered when an application tries to load malformed PKCS7 data with the d2i_PKCS7(), d2i_PKCS7_bio() or d2i_PKCS7_fp() functions. The result of the dereference is an application crash which could lead to a denial of service attack. The TLS implementation in OpenSSL does not call this function however third party applications might call these functions on untrusted data.	https://www.openssl.org/news/secadv/20230207.txt	A-OPE-OPEN-270223/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0216		
NULL Pointer Dereference	08-Feb-2023	7.5	An invalid pointer dereference on read can be triggered when an application tries to check a malformed DSA public key by the EVP_PKEY_public_check() function. This will most likely lead to an application crash. This function can be called on public keys supplied from untrusted sources which could allow an attacker to cause a denial of service attack. The TLS implementation in OpenSSL does not call this function but applications might call the function if there are additional security requirements imposed by standards such as FIPS 140-3. **CVE ID : CVE-2023-0217**	https://www.openssl.org/news/secadv/20230207.txt	A-OPE-OPEN-270223/970
NULL Pointer Dereference	08-Feb-2023	7.5	A NULL pointer can be dereferenced when signatures are being verified on PKCS7 signed or signedAndEnveloped data. In case the hash algorithm used for the signature is known to the OpenSSL library but the implementation of the hash algorithm is not available the digest	https://www.openssl.org/news/secadv/20230207.txt	A-OPE-OPEN-270223/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initialization will fail. There is a missing check for the return value from the initialization function which later leads to invalid usage of the digest API most likely leading to a crash. The unavailability of an algorithm can be caused by using FIPS enabled configuration of providers or more commonly by not loading the legacy provider. PKCS7 data is processed by the SMIME library calls and also by the time stamp (TS) library calls. The TLS implementation in OpenSSL does not call these functions however third party applications would be affected if they call these functions to verify signatures on untrusted data. **CVE ID : CVE-2023-0401**		
Vendor: Opensuse					
Product: libzypp-plugin-appdata					
Affected Version(s): * Up to (excluding) 1.0.1\\+git.20180426					
Improper Neutralization of Special Elements used in an OS	07-Feb-2023	7.8	An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in libzypp-plugin-appdata of SUSE	https://bugzilla.suse.com/show_bug.cgi?id=1206836	A-OPE-LIBZ-270223/972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			Linux Enterprise Server for SAP 15-SP3; openSUSE Leap 15.4 allows attackers that can trick users to use specially crafted REPO_ALIAS, REPO_TYPE or REPO_METADATA_PATH settings to execute code as root. This issue affects: SUSE Linux Enterprise Server for SAP 15-SP3 libzypp-plugin-appdata versions prior to 1.0.1+git.20180426. openSUSE Leap 15.4 libzypp-plugin-appdata versions prior to 1.0.1+git.20180426. **CVE ID : CVE-2023-22643**		
Vendor: openzeppelin					
Product: contracts					
Affected Version(s): From (including) 0.2.0 Up to (excluding) 0.6.1					
Improper Verification of Cryptographic Signature	03-Feb-2023	5.3	OpenZeppelin Contracts for Cairo is a library for secure smart contract development written in Cairo for StarkNet, a decentralized ZK Rollup. `is_valid_eth_signature` is missing a call to `finalize_keccak` after calling `verify_eth_signature`. As a result, any contract using `is_valid_eth_signature` from the account	https://github.com/OpenZeppelin/cairo-contracts/pull/542/commits/6d4cb750478fca2fd916f73297632f899aca9299	A-OPE-CONT-270223/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			library (such as the `EthAccount` preset) is vulnerable to a malicious sequencer. Specifically, the malicious sequencer would be able to bypass signature validation to impersonate an instance of these accounts. The issue has been patched in 0.6.1. **CVE ID : CVE-2023-23940**		
Vendor: orangescrum					
Product: orangescrum					
Affected Version(s): 2.0.11					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Feb-2023	8.1	OrangeScrum version 2.0.11 allows an authenticated external attacker to delete arbitrary local files from the server. This is possible because the application uses an unsanitized attacker-controlled parameter to construct an internal path. **CVE ID : CVE-2023-0454**	N/A	A-ORA-ORAN-270223/974
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Feb-2023	6.1	OrangeScrum version 2.0.11 allows an external attacker to obtain arbitrary user accounts from the application. This is possible because the application returns malicious user input in the response with the	N/A	A-ORA-ORAN-270223/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			content-type set to text/html. **CVE ID : CVE-2023-0624**		
Vendor: Owncloud					
Product: owncloud					
Affected Version(s): * Up to (excluding) 3.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Feb-2023	4.4	The ownCloud Android app allows ownCloud users to access, share, and edit files and folders. Prior to version 3.0, the app has an incomplete fix for a path traversal issue and is vulnerable to two bypass methods. The bypasses may lead to information disclosure when uploading the app's internal files, and to arbitrary file write when uploading plain text files (although limited by the .txt extension). Version 3.0 fixes the reported bypasses. **CVE ID : CVE-2023-24804**	https://owncloud.com/security-advisories/oc-sa-2023-001/	A-OWN-OWNC-270223/976
Affected Version(s): * Up to (including) 3.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Feb-2023	5.5	The ownCloud Android app allows ownCloud users to access, share, and edit files and folders. Version 2.21.1 of the ownCloud Android app is vulnerable to SQL injection in `FileContentProvider.kt	N/A	A-OWN-OWNC-270223/977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`. This issue can lead to information disclosure. Two databases, `filelist` and `owncloud_database`, are affected. In version 3.0, the `filelist` database was deprecated. However, injections affecting `owncloud_database` remain relevant as of version 3.0. **CVE ID : CVE-2023-23948**		
Vendor: palletsprojects					
Product: werkzeug					
Affected Version(s): * Up to (excluding) 2.2.3					
Allocation of Resources Without Limits or Throttling	14-Feb-2023	7.5	Werkzeug is a comprehensive WSGI web application library. Prior to version 2.2.3, Werkzeug's multipart form data parser will parse an unlimited number of parts, including file parts. Parts can be a small amount of bytes, but each requires CPU time to parse and may use more memory as Python data. If a request can be made to an endpoint that accesses `request.data`, `request.form`, `request.files`, or `request.get_data(parse_form_data=False)`, it can cause unexpectedly high resource usage.	https://github.com/pallets/werkzeug/commit/517cac5a804e8c4dc4ed038bb20dacd038e7a9f1, https://github.com/pallets/werkzeug/security/advisories/GHSA-xg9f-g7g7-2323	A-PAL-WERK-270223/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This allows an attacker to cause a denial of service by sending crafted multipart data to an endpoint that will parse it. The amount of CPU time required can block worker processes from handling legitimate requests. The amount of RAM required can trigger an out of memory kill of the process. Unlimited file parts can use up memory and file handles. If many concurrent requests are sent continuously, this can exhaust or kill all available workers. Version 2.2.3 contains a patch for this issue. **CVE ID : CVE-2023-25577**		
N/A	14-Feb-2023	3.5	Werkzeug is a comprehensive WSGI web application library. Browsers may allow "nameless" cookies that look like `=value` instead of `key=value`. A vulnerable browser may allow a compromised application on an adjacent subdomain to exploit this to set a cookie like `=__Host-test=bad` for another subdomain. Werkzeug prior to 2.2.3 will parse the cookie `=__Host-	https://github.com/pallets/werkzeug/security/advisories/GHSA-px8h-6qxv-m22q, https://github.com/pallets/werkzeug/commit/cf275f42acad1b5950c50ffe8ef58fe62cdce028	A-PAL-WERK-270223/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			test=bad` as __Host-test=bad`. If a Werkzeug application is running next to a vulnerable or malicious subdomain which sets such a cookie using a vulnerable browser, the Werkzeug application will see the bad cookie value but the valid cookie key. The issue is fixed in Werkzeug 2.2.3. **CVE ID : CVE-2023-23934**		
Vendor: Paloaltonetworks					
Product: cortex_xdr_agent					
Affected Version(s): From (including) 5.0 Up to (excluding) 5.0.12.22203					
N/A	08-Feb-2023	7.8	A problem with a protection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices allows a local user to execute privileged cytool commands that disable or uninstall the agent. **CVE ID : CVE-2023-0002**	https://security.paloaltonetworks.com/CVE-2023-0002	A-PAL-CORT-270223/980
Affected Version(s): From (including) 7.5 Up to (excluding) 7.5.101					
Cleartext Transmission of Sensitive Information	08-Feb-2023	6.7	An information exposure vulnerability in the Palo Alto Networks Cortex XDR agent on Windows devices allows a local system administrator to disclose the admin password for the agent in cleartext, which bad	https://security.paloaltonetworks.com/CVE-2023-0001	A-PAL-CORT-270223/981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			actors can then use to execute privileged cytool commands that disable or uninstall the agent. **CVE ID : CVE-2023-0001**		
Affected Version(s): From (including) 7.5 Up to (including) 7.5.101					
N/A	08-Feb-2023	7.8	A problem with a protection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices allows a local user to execute privileged cytool commands that disable or uninstall the agent. **CVE ID : CVE-2023-0002**	https://security.paloaltonetworks.com/CVE-2023-0002	A-PAL-CORT-270223/982
Product: cortex_xsoar					
Affected Version(s): 6.6.0					
Externally Controlled Reference to a Resource in Another Sphere	08-Feb-2023	6.5	A file disclosure vulnerability in the Palo Alto Networks Cortex XSOAR server software enables an authenticated user with access to the web interface to read local files from the server. **CVE ID : CVE-2023-0003**	https://security.paloaltonetworks.com/CVE-2023-0003	A-PAL-CORT-270223/983
Affected Version(s): 6.8.0					
Externally Controlled Reference to a Resource	08-Feb-2023	6.5	A file disclosure vulnerability in the Palo Alto Networks Cortex XSOAR server software enables an authenticated user with access to the web	https://security.paloaltonetworks.com/CVE-2023-0003	A-PAL-CORT-270223/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
in Another Sphere			interface to read local files from the server. **CVE ID : CVE-2023-0003**		
Affected Version(s): 6.9.0					
Externally Controlled Reference to a Resource in Another Sphere	08-Feb-2023	6.5	A file disclosure vulnerability in the Palo Alto Networks Cortex XSOAR server software enables an authenticated user with access to the web interface to read local files from the server. **CVE ID : CVE-2023-0003**	https://security.paloaltonetworks.com/CVE-2023-0003	A-PAL-CORT-270223/985
Affected Version(s): From (including) 6.10.0 Up to (excluding) 6.10.0.185964					
Externally Controlled Reference to a Resource in Another Sphere	08-Feb-2023	6.5	A file disclosure vulnerability in the Palo Alto Networks Cortex XSOAR server software enables an authenticated user with access to the web interface to read local files from the server. **CVE ID : CVE-2023-0003**	https://security.paloaltonetworks.com/CVE-2023-0003	A-PAL-CORT-270223/986
Vendor: parseplatform					
Product: parse-server					
Affected Version(s): * Up to (excluding) 5.4.1					
Authentication Bypass by Spoofing	03-Feb-2023	8.1	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Parse Server uses the request header `x-forwarded-for` to determine the client IP address. If	https://github.com/parse-community/parse-server/commit/e016d813e083ce6828f9abce245	A-PAR-PARS-270223/987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Parse Server doesn't run behind a proxy server, then a client can set this header and Parse Server will trust the value of the header. The incorrect client IP address will be used by various features in Parse Server. This allows to circumvent the security mechanism of the Parse Server option `masterKeyIps` by setting an allowed IP address as the `x-forwarded-for` header value. This issue has been patched in version 5.4.1. The mechanism to determine the client IP address has been rewritten. The correct IP address determination now requires to set the Parse Server option `trustProxy`. **CVE ID : CVE-2023-22474**	d15b681a224d8	
Vendor: pdfio_project					
Product: pdfio					
Affected Version(s): * Up to (excluding) 1.1.0					
Loop with Unreachable Exit Condition ('Infinite Loop')	07-Feb-2023	6.5	PDFio is a C library for reading and writing PDF files. In versions prior to 1.1.0 a denial of service (DOS) vulnerability exists in the pdfio parser. Crafted pdf files can cause the program to	https://github.com/michaelrsweet/pdfio/commit/4f10021e7ee527c1aa24853e2947e38e154d9ccb	A-PDF-PDFI-270223/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			run at 100% utilization and never terminate. The pdf which causes this crash found in testing is about 28kb in size and was discovered via fuzzing. Anyone who uses this library either as a standalone binary or as a library can be DOSed when attempting to parse this type of file. Web servers or other automated processes which rely on this code to turn pdf submissions into plaintext can be DOSed when an attacker uploads the pdf. Please see the linked GHSA for an example pdf. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-24808**		
Vendor: phpcrazy_project					
Product: phpcrazy					
Affected Version(s): 1.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Feb-2023	5.4	A vulnerability classified as problematic was found in PHPCrazy 1.1.1. This vulnerability affects unknown code of the file admin/admin.php?action=users&mode=info&user=2. The manipulation of the	N/A	A-PHP-PHPC-270223/989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument username leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-221086 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0840**		
Vendor: Phpipam					
Product: phpipam					
Affected Version(s): * Up to (excluding) 1.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Feb-2023	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository phpipam/phpipam prior to 1.5.1. **CVE ID : CVE-2023-0676**	https://github.com/phpipam/phpipam/commit/94ec73ff1d33926b75b811ded6f0b4a46088a7ec, https://huntr.dev/bounties/b72d4f0c-8a96-4b40-a031-7d469c6ab93b	A-PHP-PHPI-270223/990
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Feb-2023	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository phpipam/phpipam prior to v1.5.1. **CVE ID : CVE-2023-0677**	https://huntr.dev/bounties/d280ae81-a1c9-4a50-9aa4-f98f1f9fd2c0, https://github.com/phpipam/phpipam/commit/8fbf87e19a6	A-PHP-PHPI-270223/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				098972abc7521554db5757c3edd89	
Missing Authorization	04-Feb-2023	5.3	Improper Authorization in GitHub repository phpipam/phpipam prior to v1.5.1. **CVE ID : CVE-2023-0678**	https://github.com/phpipam/phpipam/commit/1960bd24e8a55796da066237cf11272c44bb1cc4, https://huntr.dev/bounties/8d299377-be00-46dc-bebe-3d439127982f	A-PHP-PHPI-270223/992
Vendor: Phpmyadmin					
Product: phpmyadmin					
Affected Version(s): * Up to (excluding) 4.9.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	In phpMyAdmin before 4.9.11 and 5.x before 5.2.1, an authenticated user can trigger XSS by uploading a crafted .sql file through the drag-and-drop interface. **CVE ID : CVE-2023-25727**	https://www.phpmyadmin.net/security/PMASA-2023-1/	A-PHP-PHPM-270223/993
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	In phpMyAdmin before 4.9.11 and 5.x before 5.2.1, an authenticated user can trigger XSS by uploading a crafted .sql file through the drag-and-drop interface. **CVE ID : CVE-2023-25727**	https://www.phpmyadmin.net/security/PMASA-2023-1/	A-PHP-PHPM-270223/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Phpmyfaq					
Product: phpmyfaq					
Affected Version(s): * Up to (excluding) 3.1.11					
Improper Control of Generation of Code ('Code Injection')	12-Feb-2023	9.8	Code Injection in GitHub repository thorsten/phpmyfaq prior to 3.1.11. **CVE ID : CVE-2023-0788**	https://hunter.dev/bounties/808d5452-607c-4af1-812f-26c49faf3e61, https://github.com/thorsten/phpmyfaq/commit/77b42b9d0be3990ee7389207a71528b304b03039	A-PHP-PHPM-270223/995
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Feb-2023	9.8	Command Injection in GitHub repository thorsten/phpmyfaq prior to 3.1.11. **CVE ID : CVE-2023-0789**	https://hunter.dev/bounties/d9375178-2f23-4f5d-88bd-bba3d6ba7cc5, https://github.com/thorsten/phpmyfaq/commit/40515c74815ace394ab23c6c19cbb33fd49059cb	A-PHP-PHPM-270223/996
Uncaught Exception	12-Feb-2023	8.8	Uncaught Exception in GitHub repository thorsten/phpmyfaq prior to 3.1.11. **CVE ID : CVE-2023-0790**	https://github.com/thorsten/phpmyfaq/commit/f34d84dfe551ecdd675916e45cc0606e04a0734e, https://hunt	A-PHP-PHPM-270223/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				r.dev/bounties/06af150b-b481-4248-9a48-56ded2814156	
Weak Password Requirements	12-Feb-2023	8.8	Weak Password Requirements in GitHub repository thorsten/phpmyfaq prior to 3.1.11. **CVE ID : CVE-2023-0793**	https://github.com/thorsten/phpmyfaq/commit/00c04093c671607ee06cdfd670070809460f9547, https://huntr.dev/bounties/b3881a1f-2f1e-45cb-86f3-735f66e660e9	A-PHP-PHPM-270223/998
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Feb-2023	5.4	Cross-site Scripting (XSS) - Generic in GitHub repository thorsten/phpmyfaq prior to 3.1.11. **CVE ID : CVE-2023-0787**	https://huntr.dev/bounties/87397c71-7b84-4617-a66e-fa6c73be9024, https://github.com/thorsten/phpmyfaq/commit/b76d58321a7a595eeaf4f7a30403ca6cd8506612	A-PHP-PHPM-270223/999
Improper Neutralization of Input During Web Page Generation	12-Feb-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.11.	https://github.com/thorsten/phpmyfaq/commit/26663efcb0b67e421e4ecccad8f19e7	A-PHP-PHPM-270223/1000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-0791**	106bb03ce, https://huntr.dev/bounties/7152b340-c6f3-4ac8-9f62-f764a267488d	
Improper Control of Generation of Code ('Code Injection')	12-Feb-2023	5.4	Code Injection in GitHub repository thorsten/phpmyfaq prior to 3.1.11. **CVE ID : CVE-2023-0792**	https://huntr.dev/bounties/9e21156b-ab1d-4c60-88ef-8c9f3e2feb7f, https://github.com/thorsten/phpmyfaq/commit/d8964568d69488de02f0a0a58acc822eeb5c3cb1	A-PHP-PHPM-270223/1001
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Feb-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.11. **CVE ID : CVE-2023-0794**	https://github.com/thorsten/phpmyfaq/commit/edf0f6f90d4deaf46b4fd97ae92f16c1e10a2635, https://huntr.dev/bounties/949975f1-271d-46aa-85e5-1a013cdb5efb	A-PHP-PHPM-270223/1002
Improper Neutralization of Input During	12-Feb-2023	4.8	Cross-site Scripting (XSS) - Generic in GitHub repository thorsten/phpmyfaq prior to 3.1.11.	https://github.com/thorsten/phpmyfaq/commit/ce676eb9e9	A-PHP-PHPM-270223/1003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2023-0786**	d8cb7864f36ee124e838b1ad15415f, https://hunter.dev/bounties/8c74ccab-0d1d-4c6b-a0fa-803aa65de04f	
Vendor: pickplugins					
Product: product_slider_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.13.42					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	The Product Slider for WooCommerce by PickPlugins WordPress plugin before 1.13.42 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0166**	N/A	A-PIC-PROD-270223/1004
Vendor: Pimcore					
Product: pimcore					
Affected Version(s): * Up to (excluding) 1.5.17					
Improper Neutralization of Input During Web Page Generation	14-Feb-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 1.5.17.	https://github.com/pimcore/pimcore/commit/f4050586136cb4c44e3d6042111a1b87	A-PIM-PIMC-270223/1005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-0827**	b340df95, https://hunter.dev/bounties/75bc7d07-46a7-4ed9-a405-af4fc47fb422	
Affected Version(s): * Up to (excluding) 10.5.16					
Unrestricted Upload of File with Dangerous Type	03-Feb-2023	5.4	Pimcore is an Open Source Data & Experience Management Platform: PIM, MDM, CDP, DAM, DXP/CMS & Digital Commerce. The upload functionality for updating user profile does not properly validate the file content-type, allowing any authenticated user to bypass this security check by adding a valid signature (p.e. GIF89) and sending any invalid content-type. This could allow an authenticated attacker to upload HTML files with JS content that will be executed in the context of the domain. This issue has been patched in version 10.5.16. **CVE ID : CVE-2023-23937**	https://github.com/pimcore/pimcore/commit/75a448ef8ac74424cf4e723afeb6d05f9eed872f, https://github.com/pimcore/pimcore/security/advisories/GHSA-8xv4-jj4h-qww6	A-PIM-PIMC-270223/1006
Affected Version(s): 10.5.15					
N/A	13-Feb-2023	8.8	An improper SameSite Attribute vulnerability in pimCore v10.5.15	N/A	A-PIM-PIMC-270223/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to execute arbitrary code. **CVE ID : CVE-2023-25240**		
Vendor: pinpoint					
Product: pinpoint_booking_system					
Affected Version(s): * Up to (excluding) 2.9.9.2.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Feb-2023	8.8	The Pinpoint Booking System WordPress plugin before 2.9.9.2.9 does not validate and escape one of its shortcode attributes before using it in a SQL statement, which could allow any authenticated users, such as subscriber to perform SQL Injection attacks. **CVE ID : CVE-2023-0220**	N/A	A-PIN-PINP-270223/1008
Vendor: plugin					
Product: yourchannel					
Affected Version(s): * Up to (excluding) 1.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The YourChannel WordPress plugin before 1.2.2 does not sanitize and escape some parameters, which could allow users with a role as low as Subscriber to perform Cross-Site Scripting attacks. **CVE ID : CVE-2023-0282**	N/A	A-PLU-YOUR-270223/1009
Vendor: priority-software					
Product: priority					
Affected Version(s): * Up to (excluding) 22.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Feb-2023	9.8	Priority Windows may allow Command Execution via SQL Injection using an unspecified method. **CVE ID : CVE-2023-23459**	N/A	A-PRI-PRIO-270223/1010
Affected Version(s): 19.1.0.68					
Improper Authentication	15-Feb-2023	9.8	Priority Web version 19.1.0.68, parameter manipulation on an unspecified end-point may allow authentication bypass. **CVE ID : CVE-2023-23460**	N/A	A-PRI-PRIO-270223/1011
Vendor: Progress					
Product: ws_ftp_server					
Affected Version(s): * Up to (excluding) 8.8					
Incorrect Authorization	03-Feb-2023	7.2	In Progress WS_FTP Server before 8.8, it is possible for a host administrator to elevate their privileges via the administrative interface due to insufficient authorization controls applied on user modification workflows. **CVE ID : CVE-2023-24029**	https://www.progress.com/ws_ftp, https://community.progress.com/s/article/WS-FTP-Server-Critical-Security-Product-Alert-Bulletin-January-2023?popup=true	A-PRO-WS_F-270223/1012
Vendor: Projectsend					
Product: projectsend					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) r1606					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Feb-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository projectsend/projectsend prior to r1606. **CVE ID : CVE-2023-0607**	https://github.com/projectsend/projectsend/commit/698be4ade1db6ae0eaf27c843a03ffc9683cca0a, https://huntr.dev/bounties/9294743d-7818-4264-b973-59de027d549b	A-PRO-PROJ-270223/1013
Vendor: protocol					
Product: go-bitfield					
Affected Version(s): * Up to (excluding) 1.1.0					
Improper Validation of Specified Quantity in Input	09-Feb-2023	7.5	go-bitfield is a simple bitfield package for the go language aiming to be more performant that the standard library. When feeding untrusted user input into the size parameter of `NewBitfield` and `FromBytes` functions, an attacker can trigger `panic`s. This happen when the `size` is a not a multiple of `8` or is negative. There were already a note in the `NewBitfield` documentation, however known users of this package are subject to this issue. Users are advised to	https://github.com/ipfs/go-bitfield/commit/5e1d256fe043fc4163343ccca83862c69c52e579, https://github.com/ipfs/go-bitfield/security/advisories/GHSA-2h6c-j3gf-xp9r	A-PRO-GO-B-270223/1014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade. Users unable to upgrade should ensure that `size` is a multiple of 8 before calling `NewBitfield` or `FromBytes`. **CVE ID : CVE-2023-23626**		
Product: go-unixfs					
Affected Version(s): * Up to (excluding) 0.4.3					
Uncontrolled Resource Consumption	09-Feb-2023	7.5	go-unixfs is an implementation of a unix-like filesystem on top of an ipld merkledag. Trying to read malformed HAMT sharded directories can cause panics and virtual memory leaks. If you are reading untrusted user input, an attacker can then trigger a panic. This is caused by bogus `fanout` parameter in the HAMT directory nodes. Users are advised to upgrade to version 0.4.3 to resolve this issue. Users unable to upgrade should not feed untrusted user data to the decoding functions. **CVE ID : CVE-2023-23625**	https://github.com/ipfs/go-unixfs/security/advisories/GHSA-q264-w97q-q778, https://github.com/ipfs/go-unixfs/commit/467d139a640ecee4f2e74643dafcc58bb3b54175	A-PRO-GO-U-270223/1015
Product: go-unixfsnode					
Affected Version(s): * Up to (excluding) 1.5.2					
Uncontrolled Resource	09-Feb-2023	7.5	github.com/ipfs/go-unixfsnode is an ADL IPLD prime node that wraps go-codec-	https://github.com/ipfs/go-unixfsnode/	A-PRO-GO-U-270223/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			dagpb's implementation of protobuf to enable pathing. In versions priot to 1.5.2 trying to read malformed HAMT sharded directories can cause panics and virtual memory leaks. If you are reading untrusted user input, an attacker can then trigger a panic. This is caused by bogus fanout parameter in the HAMT directory nodes. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-23631**	commit/91b3d39d33ef0cd2aff2c95d50b2329350944b68, https://github.com/ipfs/go-unixfsnode/security/advisories/GHSA-4gj3-6r43-3wfc, https://github.com/ipfs/go-unixfsnode/commit/59050ea8bc458ae55246ae09243e6e165923e076	
Vendor: pterodactyl					
Product: wings					
Affected Version(s): * Up to (excluding) 1.7.3					
Improper Link Resolution Before File Access ('Link Following')	08-Feb-2023	8.8	Wings is Pterodactyl's server control plane. Affected versions are subject to a vulnerability which can be used to create new files and directory structures on the host system that previously did not exist, potentially allowing attackers to change their resource allocations, promote their containers to privileged mode, or potentially add ssh authorized keys to allow the attacker	https://github.com/pterodactyl/wings/commit/dac9685298c3c1c49b3109fa4241aa88272b9f14, https://github.com/pterodactyl/wings/security/advisories/GHSA-p8r3-83r8-jwj5	A-PTE-WING-270223/1017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to a remote shell on the target machine. In order to use this exploit, an attacker must have an existing "server" allocated and controlled by the Wings Daemon. This vulnerability has been resolved in version `v1.11.3` of the Wings Daemon, and has been back-ported to the 1.7 release series in `v1.7.3`. Anyone running `v1.11.x` should upgrade to `v1.11.3` and anyone running `v1.7.x` should upgrade to `v1.7.3`. There are no known workarounds for this vulnerability. ### Workarounds None at this time. **CVE ID : CVE-2023-25152**		
Affected Version(s): 1.11.0					
Improper Link Resolution Before File Access ('Link Following')	08-Feb-2023	8.8	Wings is Pterodactyl's server control plane. Affected versions are subject to a vulnerability which can be used to create new files and directory structures on the host system that previously did not exist, potentially allowing attackers to change their resource allocations, promote their containers to privileged mode, or	https://github.com/pterodactyl/wings/commit/dac9685298c3c1c49b3109fa4241aa88272b9f14, https://github.com/pterodactyl/wings/security/advisories/GHSA-p8r3-83r8-jwj5	A-PTE-WING-270223/1018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially add ssh authorized keys to allow the attacker access to a remote shell on the target machine. In order to use this exploit, an attacker must have an existing "server" allocated and controlled by the Wings Daemon. This vulnerability has been resolved in version `v1.11.3` of the Wings Daemon, and has been back-ported to the 1.7 release series in `v1.7.3`. Anyone running `v1.11.x` should upgrade to `v1.11.3` and anyone running `v1.7.x` should upgrade to `v1.7.3`. There are no known workarounds for this vulnerability. ### Workarounds None at this time. **CVE ID : CVE-2023-25152**		
Improper Link Resolution Before File Access ('Link Following')	09-Feb-2023	8.2	Wings is Pterodactyl's server control plane. This vulnerability can be used to delete files and directories recursively on the host system. This vulnerability can be combined with `GHSA-p8r3-83r8-jwj5` to overwrite files on the host system. In order to use this exploit, an	https://github.com/pterodactyl/wings/commit/429ac62dba22997a278bc709df5ac00a5a25d83d, https://github.com/pterodactyl/wings/security/advisories/G	A-PTE-WING-270223/1019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker must have an existing "server" allocated and controlled by Wings. This vulnerability has been resolved in version `v1.11.4` of Wings, and has been back-ported to the 1.7 release series in `v1.7.4`. Anyone running `v1.11.x` should upgrade to `v1.11.4` and anyone running `v1.7.x` should upgrade to `v1.7.4`. There are no known workarounds for this issue. **CVE ID : CVE-2023-25168**	HSA-p8r3-83r8-jwj5, https://github.com/pterodactyl/wings/security/advisories/GHSA-66p8-j459-rq63	
Affected Version(s): 1.11.1					
Improper Link Resolution Before File Access ('Link Following')	08-Feb-2023	8.8	Wings is Pterodactyl's server control plane. Affected versions are subject to a vulnerability which can be used to create new files and directory structures on the host system that previously did not exist, potentially allowing attackers to change their resource allocations, promote their containers to privileged mode, or potentially add ssh authorized keys to allow the attacker access to a remote shell on the target machine. In order to use this exploit, an attacker	https://github.com/pterodactyl/wings/commit/dac9685298c3c1c49b3109fa4241aa88272b9f14, https://github.com/pterodactyl/wings/security/advisories/GHSA-p8r3-83r8-jwj5	A-PTE-WING-270223/1020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			must have an existing "server" allocated and controlled by the Wings Daemon. This vulnerability has been resolved in version `v1.11.3` of the Wings Daemon, and has been back-ported to the 1.7 release series in `v1.7.3`. Anyone running `v1.11.x` should upgrade to `v1.11.3` and anyone running `v1.7.x` should upgrade to `v1.7.3`. There are no known workarounds for this vulnerability. ### Workarounds None at this time. **CVE ID : CVE-2023-25152**		
Improper Link Resolution Before File Access ('Link Following')	09-Feb-2023	8.2	Wings is Pterodactyl's server control plane. This vulnerability can be used to delete files and directories recursively on the host system. This vulnerability can be combined with `GHSA-p8r3-83r8-jwj5` to overwrite files on the host system. In order to use this exploit, an attacker must have an existing "server" allocated and controlled by Wings. This vulnerability has been resolved in version `v1.11.4` of Wings, and	https://github.com/pterodactyl/wings/commit/429ac62dba22997a278bc709df5ac00a5a25d83d, https://github.com/pterodactyl/wings/security/advisories/GHSA-p8r3-83r8-jwj5, https://github.com/pterodactyl/wings/security/advisories/G	A-PTE-WING-270223/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been back-ported to the 1.7 release series in `v1.7.4`. Anyone running `v1.11.x` should upgrade to `v1.11.4` and anyone running `v1.7.x` should upgrade to `v1.7.4`. There are no known workarounds for this issue. **CVE ID : CVE-2023-25168**	HSA-66p8-j459-rq63	
Affected Version(s): 1.11.2					
Improper Link Resolution Before File Access ('Link Following')	08-Feb-2023	8.8	Wings is Pterodactyl's server control plane. Affected versions are subject to a vulnerability which can be used to create new files and directory structures on the host system that previously did not exist, potentially allowing attackers to change their resource allocations, promote their containers to privileged mode, or potentially add ssh authorized keys to allow the attacker access to a remote shell on the target machine. In order to use this exploit, an attacker must have an existing "server" allocated and controlled by the Wings Daemon. This vulnerability has been resolved in version `v1.11.3` of the Wings	https://github.com/pterodactyl/wings/commit/dac9685298c3c1c49b3109fa4241aa88272b9f14, https://github.com/pterodactyl/wings/security/advisories/GHSA-p8r3-83r8-jwj5	A-PTE-WING-270223/1022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Daemon, and has been back-ported to the 1.7 release series in `v1.7.3`. Anyone running `v1.11.x` should upgrade to `v1.11.3` and anyone running `v1.7.x` should upgrade to `v1.7.3`. There are no known workarounds for this vulnerability. ### Workarounds None at this time. **CVE ID : CVE-2023-25152**		
Improper Link Resolution Before File Access ('Link Following')	09-Feb-2023	8.2	Wings is Pterodactyl's server control plane. This vulnerability can be used to delete files and directories recursively on the host system. This vulnerability can be combined with `GHSA-p8r3-83r8-jwj5` to overwrite files on the host system. In order to use this exploit, an attacker must have an existing "server" allocated and controlled by Wings. This vulnerability has been resolved in version `v1.11.4` of Wings, and has been back-ported to the 1.7 release series in `v1.7.4`. Anyone running `v1.11.x` should upgrade to `v1.11.4` and anyone running `v1.7.x` should	https://github.com/pterodactyl/wings/commit/429ac62dba22997a278bc709df5ac00a5a25d83d, https://github.com/pterodactyl/wings/security/advisories/GHSA-p8r3-83r8-jwj5, https://github.com/pterodactyl/wings/security/advisories/GHSA-66p8-j459-rq63	A-PTE-WING-270223/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade to `v1.7.4`. There are no known workarounds for this issue. **CVE ID : CVE-2023-25168**		
Affected Version(s): 1.11.3					
Improper Link Resolution Before File Access ('Link Following')	09-Feb-2023	8.2	Wings is Pterodactyl's server control plane. This vulnerability can be used to delete files and directories recursively on the host system. This vulnerability can be combined with `GHSA-p8r3-83r8-jwj5` to overwrite files on the host system. In order to use this exploit, an attacker must have an existing "server" allocated and controlled by Wings. This vulnerability has been resolved in version `v1.11.4` of Wings, and has been back-ported to the 1.7 release series in `v1.7.4`. Anyone running `v1.11.x` should upgrade to `v1.11.4` and anyone running `v1.7.x` should upgrade to `v1.7.4`. There are no known workarounds for this issue. **CVE ID : CVE-2023-25168**	https://github.com/pterodactyl/wings/commit/429ac62dba22997a278bc709df5ac00a5a25d83d, https://github.com/pterodactyl/wings/security/advisories/GHSA-p8r3-83r8-jwj5, https://github.com/pterodactyl/wings/security/advisories/GHSA-66p8-j459-rq63	A-PTE-WING-270223/1024
Affected Version(s): From (including) 1.7.0 Up to (excluding) 1.7.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Link Resolution Before File Access ('Link Following')	09-Feb-2023	8.2	Wings is Pterodactyl's server control plane. This vulnerability can be used to delete files and directories recursively on the host system. This vulnerability can be combined with `GHSA-p8r3-83r8-jwj5` to overwrite files on the host system. In order to use this exploit, an attacker must have an existing "server" allocated and controlled by Wings. This vulnerability has been resolved in version `v1.11.4` of Wings, and has been back-ported to the 1.7 release series in `v1.7.4`. Anyone running `v1.11.x` should upgrade to `v1.11.4` and anyone running `v1.7.x` should upgrade to `v1.7.4`. There are no known workarounds for this issue. **CVE ID : CVE-2023-25168**	https://github.com/pterodactyl/wings/commit/429ac62dba22997a278bc709df5ac00a5a25d83d, https://github.com/pterodactyl/wings/security/advisories/GHSA-p8r3-83r8-jwj5, https://github.com/pterodactyl/wings/security/advisories/GHSA-66p8-j459-rq63	A-PTE-WING-270223/1025
Vendor: rafflepress					
Product: giveaways_and_contests_by_rafflepress					
Affected Version(s): * Up to (excluding) 1.11.3					
Improper Neutralization of Input During Web Page	06-Feb-2023	5.4	The Giveaways and Contests by RafflePress WordPress plugin before 1.11.3 does not validate and escape some of its shortcode	N/A	A-RAF-GIVE-270223/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0176**		
Vendor: raffle_draw_system_project					
Product: raffle_draw_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Feb-2023	9.8	Raffle Draw System v1.0 was discovered to contain multiple SQL injection vulnerabilities at save_winner.php via the ticket_id and draw parameters. **CVE ID : CVE-2023-24198**	N/A	A-RAF-RAFF-270223/1027
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Feb-2023	9.8	Raffle Draw System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at delete_ticket.php. **CVE ID : CVE-2023-24199**	N/A	A-RAF-RAFF-270223/1028
Improper Neutralization of Special Elements used in an SQL Command	06-Feb-2023	9.8	Raffle Draw System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at save_ticket.php.	N/A	A-RAF-RAFF-270223/1029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID : CVE-2023-24200**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Feb-2023	9.8	Raffle Draw System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at get_ticket.php. **CVE ID : CVE-2023-24201**	N/A	A-RAF-RAFF-270223/1030
Unrestricted Upload of File with Dangerous Type	06-Feb-2023	9.8	Raffle Draw System v1.0 was discovered to contain a local file inclusion vulnerability via the page parameter in index.php. **CVE ID : CVE-2023-24202**	N/A	A-RAF-RAFF-270223/1031
Vendor: Rapid7					
Product: metasploit					
Affected Version(s): * Up to (including) 4.21.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Feb-2023	4.8	Rapid7 Metasploit Pro versions 4.21.2 and lower suffer from a stored cross site scripting vulnerability, due to a lack of JavaScript request string sanitization. Using this vulnerability, an authenticated attacker can execute arbitrary HTML and script code in the target browser against another Metasploit Pro user using a specially crafted request. Note that in most deployments, all	https://docs.rapid7.com/release-notes/metasploit/20230130/	A-RAP-META-270223/1032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Metasploit Pro users tend to enjoy privileges equivalent to local administrator. **CVE ID : CVE-2023-0599**		
Vendor: reason-jose_project					
Product: reason-jose					
Affected Version(s): * Up to (excluding) 0.8.2					
Improper Verification of Cryptographic Signature	01-Feb-2023	9.8	reason-jose is a JOSE implementation in ReasonML and OCaml.`Jose.Jws.validate` does not check HS256 signatures. This allows tampering of JWS header and payload data if the service does not perform additional checks. Such tampering could expose applications using reason-jose to authorization bypass. Applications relying on JWS claims assertion to enforce security boundaries may be vulnerable to privilege escalation. This issue has been patched in version 0.8.2. **CVE ID : CVE-2023-23928**	https://github.com/ulrikstrid/reason-jose/commit/36cd724db3cbec121757624da49072386bd869e5	A-REA-REAS-270223/1033
Vendor: rebelcode					
Product: spotlight_social_feeds					
Affected Version(s): * Up to (excluding) 1.4.3					
Improper Neutralization of	13-Feb-2023	5.4	The Spotlight Social Feeds WordPress plugin before 1.4.3 does	N/A	A-REB-SPOT-270223/1034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0379**		
Vendor: redpanda					
Product: redpanda					
Affected Version(s): From (including) 22.1.0 Up to (excluding) 22.1.12					
Insufficiently Protected Credentials	13-Feb-2023	5.5	Redpanda before 22.3.12 discloses cleartext AWS credentials. The import functionality in the rpk binary logs an AWS Access Key ID and Secret in cleartext to standard output, allowing a local user to view the key in the console, or in Kubernetes logs if stdout output is collected. The fixed versions are 22.3.12, 22.2.10, and 22.1.12. **CVE ID : CVE-2023-24619**	https://github.com/redpanda-data/redpanda/pull/8339	A-RED-REDP-270223/1035
Affected Version(s): From (including) 22.2.0 Up to (excluding) 22.2.10					
Insufficiently Protected Credentials	13-Feb-2023	5.5	Redpanda before 22.3.12 discloses cleartext AWS credentials. The import functionality in the rpk	https://github.com/redpanda-data/redpan	A-RED-REDP-270223/1036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			binary logs an AWS Access Key ID and Secret in cleartext to standard output, allowing a local user to view the key in the console, or in Kubernetes logs if stdout output is collected. The fixed versions are 22.3.12, 22.2.10, and 22.1.12. **CVE ID : CVE-2023-24619**	da/pull/8339	
Affected Version(s): From (including) 22.3.0 Up to (excluding) 22.3.12					
Insufficiently Protected Credentials	13-Feb-2023	5.5	Redpanda before 22.3.12 discloses cleartext AWS credentials. The import functionality in the rpk binary logs an AWS Access Key ID and Secret in cleartext to standard output, allowing a local user to view the key in the console, or in Kubernetes logs if stdout output is collected. The fixed versions are 22.3.12, 22.2.10, and 22.1.12. **CVE ID : CVE-2023-24619**	https://github.com/redpanda-data/redpanda/pull/8339	A-RED-REDP-270223/1037
Vendor: responsivevoice					
Product: responsivevoice_text_to_speech					
Affected Version(s): * Up to (including) 1.7.6					
Improper Neutralization of Input	06-Feb-2023	5.4	The ResponsiveVoice Text To Speech WordPress plugin through 1.7.6 does not	N/A	A-RES-RESP-270223/1038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0070**		
Vendor: responsive_gallery_grid_project					
Product: responsive_gallery_grid					
Affected Version(s): * Up to (excluding) 2.3.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	The Responsive Gallery Grid WordPress plugin before 2.3.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0060**	N/A	A-RES-RESP-270223/1039
Vendor: rextheme					
Product: wp_vr					
Affected Version(s): * Up to (excluding) 8.2.7					
Improper Neutralization of Input During Web Page	06-Feb-2023	5.4	The WP VR WordPress plugin before 8.2.7 does not validate and escape some of its shortcode attributes before outputting them back in	N/A	A-REX-WP_V-270223/1040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0174**		
Vendor: Ruby-lang					
Product: Ruby					
Affected Version(s): * Up to (excluding) 3.2.0					
N/A	09-Feb-2023	7.5	A regular expression based DoS vulnerability in Action Dispatch <6.1.7.1 and <7.0.4.1 related to the If-None-Match header. A specially crafted HTTP If-None-Match header can cause the regular expression engine to enter a state of catastrophic backtracking, when on a version of Ruby below 3.2.0. This can cause the process to use large amounts of CPU and memory, leading to a possible DoS vulnerability All users running an affected release should either upgrade or use one of the workarounds immediately. **CVE ID : CVE-2023-22795**	https://discuss.rubyonrails.org/t/cve-2023-22795-possible-redos-based-dos-vulnerability-in-action-dispatch/82118	A-RUB-RUBY-270223/1041
Vendor: Rubyonrails					
Product: globalid					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 0.2.1 Up to (excluding) 1.0.1					
N/A	09-Feb-2023	7.5	A ReDoS based DoS vulnerability in the GlobalID <1.0.1 which could allow an attacker supplying a carefully crafted input can cause the regular expression engine to take an unexpected amount of time. All users running an affected release should either upgrade or use one of the workarounds immediately. **CVE ID : CVE-2023-22799**	https://discuss.rubyonrails.org/t/cve-2023-22799-possible-redos-based-dos-vulnerability-in-globalid/82127	A-RUB-GLOB-270223/1042
Product: rails					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.4.1					
N/A	09-Feb-2023	7.5	A regular expression based DoS vulnerability in Action Dispatch <6.0.6.1,< 6.1.7.1, and <7.0.4.1. Specially crafted cookies, in combination with a specially crafted X_FORWARDED_HOST header can cause the regular expression engine to enter a state of catastrophic backtracking. This can cause the process to use large amounts of CPU and memory, leading to a possible DoS vulnerability All users running an affected release should either upgrade or use one of	https://discuss.rubyonrails.org/t/cve-2023-22792-possible-redos-based-dos-vulnerability-in-action-dispatch/82115	A-RUB-RAIL-270223/1043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the workarounds immediately. **CVE ID : CVE-2023-22792**		
N/A	09-Feb-2023	7.5	A regular expression based DoS vulnerability in Action Dispatch <6.1.7.1 and <7.0.4.1 related to the If-None-Match header. A specially crafted HTTP If-None-Match header can cause the regular expression engine to enter a state of catastrophic backtracking, when on a version of Ruby below 3.2.0. This can cause the process to use large amounts of CPU and memory, leading to a possible DoS vulnerability All users running an affected release should either upgrade or use one of the workarounds immediately. **CVE ID : CVE-2023-22795**	https://discuss.rubyonrails.org/t/cve-2023-22795-possible-redos-based-dos-vulnerability-in-action-dispatch/82118	A-RUB-RAIL-270223/1044
URL Redirection to Untrusted Site ('Open Redirect')	09-Feb-2023	6.1	An open redirect vulnerability is fixed in Rails 7.0.4.1 with the new protection against open redirects from calling redirect_to with untrusted user input. In prior versions the developer was fully responsible for only providing trusted input. However the check	N/A	A-RUB-RAIL-270223/1045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			introduced could allow an attacker to bypass with a carefully crafted URL resulting in an open redirect vulnerability. **CVE ID : CVE-2023-22797**		
Affected Version(s): From (including) 6.1.0 Up to (excluding) 6.1.7.1					
N/A	09-Feb-2023	7.5	A regular expression based DoS vulnerability in Action Dispatch <6.0.6.1,< 6.1.7.1, and <7.0.4.1. Specially crafted cookies, in combination with a specially crafted X_FORWARDED_HOST header can cause the regular expression engine to enter a state of catastrophic backtracking. This can cause the process to use large amounts of CPU and memory, leading to a possible DoS vulnerability All users running an affected release should either upgrade or use one of the workarounds immediately. **CVE ID : CVE-2023-22792**	https://discuss.rubyonrails.org/t/cve-2023-22792-possible-redos-based-dos-vulnerability-in-action-dispatch/82115	A-RUB-RAIL-270223/1046
N/A	09-Feb-2023	7.5	A regular expression based DoS vulnerability in Action Dispatch <6.1.7.1 and <7.0.4.1 related to the If-None-Match header. A specially crafted HTTP	https://discuss.rubyonrails.org/t/cve-2023-22795-possible-redos-based-	A-RUB-RAIL-270223/1047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If-None-Match header can cause the regular expression engine to enter a state of catastrophic backtracking, when on a version of Ruby below 3.2.0. This can cause the process to use large amounts of CPU and memory, leading to a possible DoS vulnerability All users running an affected release should either upgrade or use one of the workarounds immediately. **CVE ID : CVE-2023-22795**	dos-vulnerability-in-action-dispatch/82118	
Affected Version(s): * Up to (excluding) 5.2.0					
Cross-Site Request Forgery (CSRF)	02-Feb-2023	6.5	Clockwork Web before 0.1.2, when Rails before 5.2 is used, allows CSRF. **CVE ID : CVE-2023-25015**	https://github.com/ankane/clockwork_web/commit/ec2896503ee231588547c2fad4cb93a94e78f857, https://github.com/ankane/clockwork_web/issues/4, https://github.com/ankane/clockwork_web/compare/v0.1.1...v0.1.2	A-RUB-RAIL-270223/1048
Affected Version(s): From (including) 3.0.0 Up to (excluding) 6.0.6.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Feb-2023	7.5	A regular expression based DoS vulnerability in Action Dispatch <6.0.6.1,< 6.1.7.1, and <7.0.4.1. Specially crafted cookies, in combination with a specially crafted X_FORWARDED_HOST header can cause the regular expression engine to enter a state of catastrophic backtracking. This can cause the process to use large amounts of CPU and memory, leading to a possible DoS vulnerability All users running an affected release should either upgrade or use one of the workarounds immediately. **CVE ID : CVE-2023-22792**	https://discuss.rubyonrails.org/t/cve-2023-22792-possible-redos-based-dos-vulnerability-in-action-dispatch/82115	A-RUB-RAIL-270223/1049
Vendor: Ruckuswireless					
Product: ruckus_wireless_admin					
Affected Version(s): * Up to (including) 10.4					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	A-RUC-RUCK-270223/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Samsung					
Product: bixby_vision					
Affected Version(s): * Up to (excluding) 3.7.70.17					
Improper Input Validation	09-Feb-2023	3.3	Improper input validation in Bixby Vision prior to version 3.7.70.17 allows attacker to access data of Bixby Vision. **CVE ID : CVE-2023-21431**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=01	A-SAM-BIXB-270223/1051
Product: cloud					
Affected Version(s): * Up to (excluding) 5.3.0.32					
Exposure of Resource to Wrong Sphere	09-Feb-2023	3.3	Improper access control vulnerabilities in Samsung Cloud prior to version 5.3.0.32 allows local attackers to access information with Samsung Cloud's privilege via implicit intent. **CVE ID : CVE-2023-21447**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=02	A-SAM-CLOU-270223/1052
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Feb-2023	3.3	Path traversal vulnerability in Samsung Cloud prior to version 5.3.0.32 allows attacker to access specific png file. **CVE ID : CVE-2023-21448**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=02	A-SAM-CLOU-270223/1053
Product: flow					
Affected Version(s): * Up to (excluding) 4.9.04					
Inadequate Encryption Strength	09-Feb-2023	8.8	Improper cryptographic implementation in Samsung Flow for Android prior to	https://security.samsungmobile.com/serviceWeb.smsb?year=	A-SAM-FLOW-270223/1054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 4.9.04 allows adjacent attackers to decrypt encrypted messages or inject commands. **CVE ID : CVE-2023-21443**	2023&month=02	
Affected Version(s): * Up to (excluding) 4.9.14.0					
Inadequate Encryption Strength	09-Feb-2023	8.8	Improper cryptographic implementation in Samsung Flow for PC 4.9.14.0 allows adjacent attackers to decrypt encrypted messages or inject commands. **CVE ID : CVE-2023-21444**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=02	A-SAM-FLOW-270223/1055
Product: galaxy_store					
Affected Version(s): * Up to (excluding) 4.5.49.8					
Incorrect Default Permissions	09-Feb-2023	7.8	Improper access control vulnerability in Galaxy Store prior to version 4.5.49.8 allows local attackers to install applications from Galaxy Store. **CVE ID : CVE-2023-21433**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=01	A-SAM-GALA-270223/1056
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Feb-2023	6.1	Improper input validation vulnerability in Galaxy Store prior to version 4.5.49.8 allows local attackers to execute JavaScript by launching a web page. **CVE ID : CVE-2023-21434**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=01	A-SAM-GALA-270223/1057
Product: one_hand_operation_\+					
Affected Version(s): * Up to (excluding) 6.1.21					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	09-Feb-2023	2.1	Missing Authorization vulnerability in One Hand Operation + prior to version 6.1.21 allows multi-users to access owner's widget without authorization via gesture setting. **CVE ID : CVE-2023-21450**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=02	A-SAM-ONE_-270223/1058
Product: smart_things					
Affected Version(s): * Up to (excluding) 1.7.93					
N/A	09-Feb-2023	7.8	Improper access control vulnerabilities in Smart Things prior to 1.7.93 allows to attacker to invite others without authorization of the owner. **CVE ID : CVE-2023-21432**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=01	A-SAM-SMAR-270223/1059
Vendor: SAP					
Product: businessobjects_business_intelligence_platform					
Affected Version(s): 420					
Unrestricted Upload of File with Dangerous Type	14-Feb-2023	9.1	SAP BusinessObjects Business Intelligence Platform (CMC) - versions 420, 430, allows an authenticated admin user to upload malicious code that can be executed by the application over the network. On successful exploitation, attacker can perform operations that may completely compromise the application causing high impact on confidentiality, integrity	https://launchpad.support.sap.com/#/notes/3256787, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-270223/1060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and availability of the application. **CVE ID : CVE-2023-24530**		
Exposure of Sensitive Information to an Unauthorized Actor	14-Feb-2023	7.1	SAP BusinessObjects Business Intelligence platform - versions 420, 430, allows an authenticated attacker to access sensitive information which is otherwise restricted. On successful exploitation, there could be a high impact on confidentiality and limited impact on integrity of the application. **CVE ID : CVE-2023-0020**	https://launchpad.support.sap.com/#/notes/3263135, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-270223/1061
Affected Version(s): 430					
Unrestricted Upload of File with Dangerous Type	14-Feb-2023	9.1	SAP BusinessObjects Business Intelligence Platform (CMC) - versions 420, 430, allows an authenticated admin user to upload malicious code that can be executed by the application over the network. On successful exploitation, attacker can perform operations that may completely compromise the application causing high impact on confidentiality, integrity and availability of the application.	https://launchpad.support.sap.com/#/notes/3256787, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-270223/1062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24530		
Exposure of Sensitive Information to an Unauthorized Actor	14-Feb-2023	7.1	SAP BusinessObjects Business Intelligence platform - versions 420, 430, allows an authenticated attacker to access sensitive information which is otherwise restricted. On successful exploitation, there could be a high impact on confidentiality and limited impact on integrity of the application. **CVE ID : CVE-2023-0020**	https://launchpad.support.sap.com/#/notes/3263135, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-270223/1063
Product: business_objects_business_intelligence_platform					
Affected Version(s): 430					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	In SAP BusinessObjects Business Intelligence (Web Intelligence user interface) - version 430, some calls return json with wrong content type in the header of the response. As a result, a custom application that calls directly the jsp of Web Intelligence DHTML may be vulnerable to XSS attacks. On successful exploitation an attacker can cause a low impact on integrity of the application. **CVE ID : CVE-2023-23856**	https://launchpad.support.sap.com/#/notes/3263863, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-270223/1064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: business_planning_and_consolidation					
Affected Version(s): 200					
Unrestricted Upload of File with Dangerous Type	14-Feb-2023	5.4	SAP Business Planning and Consolidation - versions 200, 300, allows an attacker with business authorization to upload any files (including web pages) without the proper file format validation. If other users visit the uploaded malicious web page, the attacker may perform actions on behalf of the users without their consent impacting the confidentiality and integrity of the system. **CVE ID : CVE-2023-23851**	https://launchpad.support.sap.com/#/notes/3275841, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-270223/1065
Affected Version(s): 300					
Unrestricted Upload of File with Dangerous Type	14-Feb-2023	5.4	SAP Business Planning and Consolidation - versions 200, 300, allows an attacker with business authorization to upload any files (including web pages) without the proper file format validation. If other users visit the uploaded malicious web page, the attacker may perform actions on behalf of the users without their consent impacting the confidentiality and integrity of the system.	https://launchpad.support.sap.com/#/notes/3275841, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-270223/1066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23851		
Product: customer_relationship_management_webclient_ui					
Affected Version(s): 7.00					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	SAP CRM WebClient UI - versions WEBCUIF 748, 800, 801, S4FND 102, 103, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an authenticated attacker can cause limited impact on confidentiality of the application. **CVE ID : CVE-2023-24525**	https://launchpad.support.sap.com/#/notes/2788178, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-270223/1067
Affected Version(s): 7.01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	SAP CRM WebClient UI - versions WEBCUIF 748, 800, 801, S4FND 102, 103, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an authenticated attacker can cause limited impact on confidentiality of the application. **CVE ID : CVE-2023-24525**	https://launchpad.support.sap.com/#/notes/2788178, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-270223/1068
Affected Version(s): 7.02					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	SAP CRM WebClient UI - versions WEBCUIF 748, 800, 801, S4FND 102, 103, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an authenticated attacker can cause limited impact on confidentiality of the application. **CVE ID : CVE-2023-24525**	https://launchpad.support.sap.com/#/notes/2788178, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-270223/1069
Affected Version(s): 7.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	SAP CRM WebClient UI - versions WEBCUIF 748, 800, 801, S4FND 102, 103, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an authenticated attacker can cause limited impact on confidentiality of the application. **CVE ID : CVE-2023-24525**	https://launchpad.support.sap.com/#/notes/2788178, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-270223/1070
Affected Version(s): 7.40					
Improper Neutralization of Input During Web Page	14-Feb-2023	5.4	SAP CRM WebClient UI - versions WEBCUIF 748, 800, 801, S4FND 102, 103, does not sufficiently encode user-controlled inputs,	https://launchpad.support.sap.com/#/notes/2788178, https://ww	A-SAP-CUST-270223/1071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an authenticated attacker can cause limited impact on confidentiality of the application. **CVE ID : CVE-2023-24525**	w.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 7.48					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	SAP CRM WebClient UI - versions WEBCUIF 748, 800, 801, S4FND 102, 103, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an authenticated attacker can cause limited impact on confidentiality of the application. **CVE ID : CVE-2023-24525**	https://launchpad.support.sap.com/#/notes/2788178, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-270223/1072
Affected Version(s): 7.50					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	SAP CRM WebClient UI - versions WEBCUIF 748, 800, 801, S4FND 102, 103, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an authenticated attacker can cause	https://launchpad.support.sap.com/#/notes/2788178, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-CUST-270223/1073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			limited impact on confidentiality of the application. **CVE ID : CVE-2023-24525**	c68f7e60039b.html	
Affected Version(s): 7.52					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	SAP CRM WebClient UI - versions WEBCUIF 748, 800, 801, S4FND 102, 103, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an authenticated attacker can cause limited impact on confidentiality of the application. **CVE ID : CVE-2023-24525**	https://launchpad.support.sap.com/#/notes/2788178, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-270223/1074
Affected Version(s): 8.00					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	SAP CRM WebClient UI - versions WEBCUIF 748, 800, 801, S4FND 102, 103, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an authenticated attacker can cause limited impact on confidentiality of the application. **CVE ID : CVE-2023-24525**	https://launchpad.support.sap.com/#/notes/2788178, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-270223/1075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 8.01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	SAP CRM WebClient UI - versions WEBCUIF 748, 800, 801, S4FND 102, 103, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an authenticated attacker can cause limited impact on confidentiality of the application. **CVE ID : CVE-2023-24525**	https://launchpad.support.sap.com/#/notes/2788178, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-270223/1076
Product: fiori					
Affected Version(s): 600					
Missing Authorization	14-Feb-2023	6.5	SAP Fiori apps for Travel Management in SAP ERP (My Travel Requests) - version 600, allows an authenticated attacker to exploit a certain misconfigured application endpoint to view sensitive data. This endpoint is normally exposed over the network and successful exploitation can lead to exposure of data like travel documents. **CVE ID : CVE-2023-24528**	https://launchpad.support.sap.com/#/notes/3290901, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-FIOR-270223/1077
Product: grc_process_control					
Affected Version(s): v1100_700					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	14-Feb-2023	6.5	In SAP GRC (Process Control) - versions GRCFND_A V1200, GRCFND_A V8100, GRCPINW V1100_700, GRCPINW V1100_731, GRCPINW V1200_750, remote-enabled function module in the proprietary SAP solution enables an authenticated attacker with minimal privileges to access all the confidential data stored in the database. Successful exploitation of this vulnerability can expose user credentials from client-specific tables of the database, leading to high impact on confidentiality. **CVE ID : CVE-2023-0019**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-GRC_-270223/1078
Affected Version(s): v1100_731					
Missing Authorization	14-Feb-2023	6.5	In SAP GRC (Process Control) - versions GRCFND_A V1200, GRCFND_A V8100, GRCPINW V1100_700, GRCPINW V1100_731, GRCPINW V1200_750, remote-enabled function module in the proprietary SAP solution enables an authenticated attacker with minimal privileges to access all the confidential data stored in the database. Successful exploitation	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-GRC_-270223/1079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can expose user credentials from client-specific tables of the database, leading to high impact on confidentiality. **CVE ID : CVE-2023-0019**		
Affected Version(s): v1200					
Missing Authorization	14-Feb-2023	6.5	In SAP GRC (Process Control) - versions GRCFND_A V1200, GRCFND_A V8100, GRCPINW V1100_700, GRCPINW V1100_731, GRCPINW V1200_750, remote-enabled function module in the proprietary SAP solution enables an authenticated attacker with minimal privileges to access all the confidential data stored in the database. Successful exploitation of this vulnerability can expose user credentials from client-specific tables of the database, leading to high impact on confidentiality. **CVE ID : CVE-2023-0019**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-GRC_-270223/1080
Affected Version(s): v1200_750					
Missing Authorization	14-Feb-2023	6.5	In SAP GRC (Process Control) - versions GRCFND_A V1200, GRCFND_A V8100, GRCPINW V1100_700, GRCPINW V1100_731, GRCPINW V1200_750,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-GRC_-270223/1081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote-enabled function module in the proprietary SAP solution enables an authenticated attacker with minimal privileges to access all the confidential data stored in the database. Successful exploitation of this vulnerability can expose user credentials from client-specific tables of the database, leading to high impact on confidentiality. **CVE ID : CVE-2023-0019**	c68f7e60039b.html	
Affected Version(s): v8100					
Missing Authorization	14-Feb-2023	6.5	In SAP GRC (Process Control) - versions GRCFND_A V1200, GRCFND_A V8100, GRCPINW V1100_700, GRCPINW V1100_731, GRCPINW V1200_750, remote-enabled function module in the proprietary SAP solution enables an authenticated attacker with minimal privileges to access all the confidential data stored in the database. Successful exploitation of this vulnerability can expose user credentials from client-specific tables of the database, leading to high impact on confidentiality.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-GRC_-270223/1082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0019		
Product: host_agent					
Affected Version(s): 7.21					
Exposure of Resource to Wrong Sphere	14-Feb-2023	8.8	An attacker authenticated as a non-admin user with local access to a server port assigned to the SAP Host Agent (Start Service) - versions 7.21, 7.22, can submit a crafted ConfigureOutsideDiscovery request with an operating system command which will be executed with administrator privileges. The OS command can read or modify any user or system data and can make the system unavailable. **CVE ID : CVE-2023-24523**	https://launchpad.support.sap.com/#/notes/3285757, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-HOST-270223/1083
Affected Version(s): 7.22					
Exposure of Resource to Wrong Sphere	14-Feb-2023	8.8	An attacker authenticated as a non-admin user with local access to a server port assigned to the SAP Host Agent (Start Service) - versions 7.21, 7.22, can submit a crafted ConfigureOutsideDiscovery request with an operating system command which will be executed with	https://launchpad.support.sap.com/#/notes/3285757, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-HOST-270223/1084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator privileges. The OS command can read or modify any user or system data and can make the system unavailable. **CVE ID : CVE-2023-24523**		
Product: netweaver_application_server_abap					
Affected Version(s): 700					
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	An unauthenticated attacker in AP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, can craft a link which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. Vulnerability has no direct impact on availability. **CVE ID : CVE-2023-23853**	https://launchpad.support.sap.com/#/notes/3271227, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1085
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (Business Server Pages) - versions 700, 701, 702, 731, 740, allows an unauthenticated user to alter the current session of the user by	https://launchpad.support.sap.com/#/notes/3269118, https://www.sap.com/documents/2022/02/fa8	A-SAP-NETW-270223/1086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24522**	65ea4-167e-0010-bca6-c68f7e60039b.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS ABAP (BSP Framework) application - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allow an unauthenticated attacker to inject the code that can be executed by the application over the network. On successful exploitation it can gain access to the sensitive information which leads to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-25614**	https://launchpad.support.sap.com/#/notes/3274585, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1087
Missing Authorization	14-Feb-2023	5.4	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, does not perform necessary authorization checks for an authenticated	https://launchpad.support.sap.com/#/notes/3287291, https://www.sap.com/documents/2022/02/fa865ea4-167e-	A-SAP-NETW-270223/1088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user, resulting in escalation of privileges. **CVE ID : CVE-2023-23854**	0010-bca6-c68f7e60039b.html	
Affected Version(s): 701					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (Business Server Pages) - versions 700, 701, 702, 731, 740, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24522**	https://launchpad.support.sap.com/#/notes/3269118, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1089
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS ABAP (BSP Framework) application - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allow an unauthenticated attacker to inject the code that can be executed by the application over the network. On successful exploitation it can gain access to the sensitive information which leads to a limited impact on the	https://launchpad.support.sap.com/#/notes/3274585, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality and the integrity of the application. **CVE ID : CVE-2023-25614**		
Missing Authorization	14-Feb-2023	5.4	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. **CVE ID : CVE-2023-23854**	https://launchpad.support.sap.com/#/notes/3287291, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1091
Affected Version(s): 702					
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	An unauthenticated attacker in AP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, can craft a link which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. Vulnerability has no direct impact on availability. **CVE ID : CVE-2023-23853**	https://launchpad.support.sap.com/#/notes/3271227, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (Business Server Pages) - versions 700, 701, 702, 731, 740, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24522**	https://launchpad.support.sap.com/#/notes/3269118, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1093
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS ABAP (BSP Framework) application - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allow an unauthenticated attacker to inject the code that can be executed by the application over the network. On successful exploitation it can gain access to the sensitive information which leads to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-25614**	https://launchpad.support.sap.com/#/notes/3274585, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	14-Feb-2023	5.4	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. **CVE ID : CVE-2023-23854**	https://launchpad.support.sap.com/#/notes/3287291, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1095
Affected Version(s): 731					
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	An unauthenticated attacker in AP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, can craft a link which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. Vulnerability has no direct impact on availability. **CVE ID : CVE-2023-23853**	https://launchpad.support.sap.com/#/notes/3271227, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1096
Improper Neutralization of Input During Web Page	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (Business Server Pages) - versions 700, 701, 702, 731, 740, allows an	https://launchpad.support.sap.com/#/notes/3269118, https://ww	A-SAP-NETW-270223/1097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24522**	w.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS ABAP (BSP Framework) application - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allow an unauthenticated attacker to inject the code that can be executed by the application over the network. On successful exploitation it can gain access to the sensitive information which leads to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-25614**	https://launchpad.support.sap.com/#/notes/3274585, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1098
Missing Authorization	14-Feb-2023	5.4	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, does not perform necessary	https://launchpad.support.sap.com/#/notes/3287291, https://www.sap.com/d	A-SAP-NETW-270223/1099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authorization checks for an authenticated user, resulting in escalation of privileges. **CVE ID : CVE-2023-23854**	ocuments/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 740					
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	An unauthenticated attacker in AP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, can craft a link which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. Vulnerability has no direct impact on availability. **CVE ID : CVE-2023-23853**	https://launchpad.support.sap.com/#/notes/3271227, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1100
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input validation, SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to send a crafted URL to a user, and by clicking the URL, the tricked user accesses SAP and might	https://launchpad.support.sap.com/#/notes/3293786, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be directed with the response to somewhere out-side SAP and enter sensitive data. This could cause a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-23858**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can be used to read or modify some sensitive information. **CVE ID : CVE-2023-23859**	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1102
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a link, which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the victim to a phishing attack. **CVE ID : CVE-2023-23860**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (Business Server Pages) - versions 700, 701, 702, 731, 740, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24522**	https://launchpad.support.sap.com/#/notes/3269118, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1104
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS ABAP (BSP Framework) application - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allow an unauthenticated attacker to inject the code that can be executed by the application over the network. On successful exploitation it can gain access to the sensitive information which leads to a limited impact on the confidentiality and the	https://launchpad.support.sap.com/#/notes/3274585, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity of the application. **CVE ID : CVE-2023-25614**		
Missing Authorization	14-Feb-2023	5.4	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. **CVE ID : CVE-2023-23854**	https://launchpad.support.sap.com/#/notes/3287291, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1106
Affected Version(s): 750					
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	An unauthenticated attacker in AP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, can craft a link which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. Vulnerability has no direct impact on availability. **CVE ID : CVE-2023-23853**	https://launchpad.support.sap.com/#/notes/3271227, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input validation, SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to send a crafted URL to a user, and by clicking the URL, the tricked user accesses SAP and might be directed with the response to somewhere out-side SAP and enter sensitive data. This could cause a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-23858**	https://launchpad.support.sap.com/#/notes/3293786, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1108
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can be used to read or modify some sensitive information. **CVE ID : CVE-2023-23859**	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1109
URL Redirection to	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740,	https://launchpad.support.sap.com/#	A-SAP-NETW-270223/1110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Site ('Open Redirect')			750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a link, which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. **CVE ID : CVE-2023-23860**	/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS ABAP (BSP Framework) application - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allow an unauthenticated attacker to inject the code that can be executed by the application over the network. On successful exploitation it can gain access to the sensitive information which leads to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-25614**	https://launchpad.support.sap.com/#/notes/3274585, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1111
Missing Authorization	14-Feb-2023	5.4	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750,	https://launchpad.support.sap.com/#/notes/3287291,	A-SAP-NETW-270223/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			751, 752, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. **CVE ID : CVE-2023-23854**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 751					
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	An unauthenticated attacker in AP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, can craft a link which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. Vulnerability has no direct impact on availability. **CVE ID : CVE-2023-23853**	https://launchpad.support.sap.com/#/notes/3271227, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1113
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input validation, SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to send a crafted URL to a user, and by clicking the URL,	https://launchpad.support.sap.com/#/notes/3293786, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-NETW-270223/1114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the tricked user accesses SAP and might be directed with the response to somewhere out-side SAP and enter sensitive data. This could cause a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-23858**	c68f7e60039b.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can be used to read or modify some sensitive information. **CVE ID : CVE-2023-23859**	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1115
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a link, which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information or expose the victim to a phishing attack. **CVE ID : CVE-2023-23860**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS ABAP (BSP Framework) application - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allow an unauthenticated attacker to inject the code that can be executed by the application over the network. On successful exploitation it can gain access to the sensitive information which leads to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-25614**	https://launchpad.support.sap.com/#/notes/3274585, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1117
Missing Authorization	14-Feb-2023	5.4	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. **CVE ID : CVE-2023-23854**	https://launchpad.support.sap.com/#/notes/3287291, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1118
Affected Version(s): 752					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	An unauthenticated attacker in AP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, can craft a link which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. Vulnerability has no direct impact on availability. **CVE ID : CVE-2023-23853**	https://launchpad.support.sap.com/#/notes/3271227, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1119
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input validation, SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to send a crafted URL to a user, and by clicking the URL, the tricked user accesses SAP and might be directed with the response to somewhere out-side SAP and enter sensitive data. This could cause a limited impact on confidentiality and	https://launchpad.support.sap.com/#/notes/3293786, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity of the application. **CVE ID : CVE-2023-23858**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can be used to read or modify some sensitive information. **CVE ID : CVE-2023-23859**	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1121
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a link, which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. **CVE ID : CVE-2023-23860**	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1122
Improper Neutralization of	14-Feb-2023	6.1	SAP NetWeaver AS ABAP (BSP Framework) application - versions	https://launchpad.support.sap.com/#	A-SAP-NETW-270223/1123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allow an unauthenticated attacker to inject the code that can be executed by the application over the network. On successful exploitation it can gain access to the sensitive information which leads to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-25614**	/notes/3274585, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Missing Authorization	14-Feb-2023	5.4	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. **CVE ID : CVE-2023-23854**	https://launchpad.support.sap.com/#/notes/3287291, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1124
Affected Version(s): 753					
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	An unauthenticated attacker in AP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, can craft a link	https://launchpad.support.sap.com/#/notes/3271227, https://www.sap.com/documents/2022/02/fa8	A-SAP-NETW-270223/1125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. Vulnerability has no direct impact on availability. **CVE ID : CVE-2023-23853**	65ea4-167e-0010-bca6-c68f7e60039b.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input validation, SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to send a crafted URL to a user, and by clicking the URL, the tricked user accesses SAP and might be directed with the response to somewhere out-side SAP and enter sensitive data. This could cause a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-23858**	https://launchpad.support.sap.com/#/notes/3293786, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1126
Improper Neutralization of Input During Web Page	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an	https://launchpad.support.sap.com/#/notes/3268959, https://ww	A-SAP-NETW-270223/1127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			unauthenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can be used to read or modify some sensitive information. **CVE ID : CVE-2023-23859**	w.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a link, which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. **CVE ID : CVE-2023-23860**	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1128
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS ABAP (BSP Framework) application - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allow an unauthenticated attacker to inject the code that can be executed by the application over the network. On successful exploitation it can gain access to the sensitive	https://launchpad.support.sap.com/#/notes/3274585, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information which leads to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-25614**		
Affected Version(s): 754					
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	An unauthenticated attacker in AP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, can craft a link which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. Vulnerability has no direct impact on availability. **CVE ID : CVE-2023-23853**	https://launchpad.support.sap.com/#/notes/3271227, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1130
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input validation, SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to send a crafted URL to a user, and by clicking the URL,	https://launchpad.support.sap.com/#/notes/3293786, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-NETW-270223/1131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the tricked user accesses SAP and might be directed with the response to somewhere out-side SAP and enter sensitive data. This could cause a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-23858**	c68f7e60039b.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can be used to read or modify some sensitive information. **CVE ID : CVE-2023-23859**	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1132
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a link, which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information or expose the victim to a phishing attack. **CVE ID : CVE-2023-23860**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS ABAP (BSP Framework) application - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allow an unauthenticated attacker to inject the code that can be executed by the application over the network. On successful exploitation it can gain access to the sensitive information which leads to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-25614**	https://launchpad.support.sap.com/#/notes/3274585, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1134
Affected Version(s): 755					
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	An unauthenticated attacker in AP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, can craft a link which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or	https://launchpad.support.sap.com/#/notes/3271227, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modify some sensitive information or expose the victim to a phishing attack. Vulnerability has no direct impact on availability. **CVE ID : CVE-2023-23853**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input validation, SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to send a crafted URL to a user, and by clicking the URL, the tricked user accesses SAP and might be directed with the response to somewhere out-side SAP and enter sensitive data. This could cause a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-23858**	https://launchpad.support.sap.com/#/notes/3293786, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1136
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-NETW-270223/1137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used to read or modify some sensitive information. **CVE ID : CVE-2023-23859**	c68f7e60039b.html	
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a link, which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. **CVE ID : CVE-2023-23860**	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1138
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS ABAP (BSP Framework) application - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allow an unauthenticated attacker to inject the code that can be executed by the application over the network. On successful exploitation it can gain access to the sensitive information which leads to a limited impact on the confidentiality and the	https://launchpad.support.sap.com/#/notes/3274585, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity of the application. **CVE ID : CVE-2023-25614**		
Affected Version(s): 756					
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	An unauthenticated attacker in AP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, can craft a link which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. Vulnerability has no direct impact on availability. **CVE ID : CVE-2023-23853**	https://launchpad.support.sap.com/#/notes/3271227, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1140
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input validation, SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to send a crafted URL to a user, and by clicking the URL, the tricked user accesses SAP and might be directed with the response to somewhere	https://launchpad.support.sap.com/#/notes/3293786, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out-side SAP and enter sensitive data. This could cause a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-23858**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can be used to read or modify some sensitive information. **CVE ID : CVE-2023-23859**	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1142
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a link, which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack.	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23860		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS ABAP (BSP Framework) application - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allow an unauthenticated attacker to inject the code that can be executed by the application over the network. On successful exploitation it can gain access to the sensitive information which leads to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-25614**	https://launchpad.support.sap.com/#/notes/3274585, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1144
Affected Version(s): 757					
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	An unauthenticated attacker in AP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, can craft a link which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. Vulnerability	https://launchpad.support.sap.com/#/notes/3271227, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has no direct impact on availability. **CVE ID : CVE-2023-23853**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input validation, SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to send a crafted URL to a user, and by clicking the URL, the tricked user accesses SAP and might be directed with the response to somewhere out-side SAP and enter sensitive data. This could cause a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-23858**	https://launchpad.support.sap.com/#/notes/3293786, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1146
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can be used to read or modify some sensitive information.	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23859		
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a link, which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. **CVE ID : CVE-2023-23860**	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1148
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS ABAP (BSP Framework) application - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allow an unauthenticated attacker to inject the code that can be executed by the application over the network. On successful exploitation it can gain access to the sensitive information which leads to a limited impact on the confidentiality and the integrity of the application.	https://launchpad.support.sap.com/#/notes/3274585, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25614		
Affected Version(s): 789					
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	An unauthenticated attacker in AP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, can craft a link which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. Vulnerability has no direct impact on availability. **CVE ID : CVE-2023-23853**	https://launchpad.support.sap.com/#/notes/3271227, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1150
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can be used to read or modify some sensitive information. **CVE ID : CVE-2023-23859**	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a link, which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. **CVE ID : CVE-2023-23860**	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1152
Affected Version(s): 790					
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	An unauthenticated attacker in AP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, can craft a link which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. Vulnerability has no direct impact on availability. **CVE ID : CVE-2023-23853**	https://launchpad.support.sap.com/#/notes/3271227, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can be used to read or modify some sensitive information. **CVE ID : CVE-2023-23859**	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1154
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	6.1	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a link, which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. **CVE ID : CVE-2023-23860**	https://launchpad.support.sap.com/#/notes/3268959, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1155
Product: netweaver_as_abap_business_server_pages					
Affected Version(s): 7.00					
Improper Neutralization of Input During	14-Feb-2023	6.1	Due to lack of proper input validation, BSP application (CRM_BSP_FRAME) - versions 700, 701, 702,	https://launchpad.support.sap.com/#/notes/3282663,	A-SAP-NETW-270223/1156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, allow malicious inputs from untrusted sources, which can be leveraged by an attacker to execute a Reflected Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to hijack a user session, read and modify some sensitive information. **CVE ID : CVE-2023-24529**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 7.01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to lack of proper input validation, BSP application (CRM_BSP_FRAME) - versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, allow malicious inputs from untrusted sources, which can be leveraged by an attacker to execute a Reflected Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to hijack a user session, read and modify some sensitive information. **CVE ID : CVE-2023-24529**	https://launchpad.support.sap.com/#/notes/3282663, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1157
Affected Version(s): 7.02					
Improper Neutralization of	14-Feb-2023	6.1	Due to lack of proper input validation, BSP application	https://launchpad.support.sap.com/#	A-SAP-NETW-270223/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			(CRM_BSP_FRAME) - versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, allow malicious inputs from untrusted sources, which can be leveraged by an attacker to execute a Reflected Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to hijack a user session, read and modify some sensitive information. **CVE ID : CVE-2023-24529**	/notes/3282663, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 7.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to lack of proper input validation, BSP application (CRM_BSP_FRAME) - versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, allow malicious inputs from untrusted sources, which can be leveraged by an attacker to execute a Reflected Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to hijack a user session, read and modify some sensitive information. **CVE ID : CVE-2023-24529**	https://launchpad.support.sap.com/#/notes/3282663, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1159
Affected Version(s): 7.40					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to lack of proper input validation, BSP application (CRM_BSP_FRAME) - versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, allow malicious inputs from untrusted sources, which can be leveraged by an attacker to execute a Reflected Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to hijack a user session, read and modify some sensitive information. **CVE ID : CVE-2023-24529**	https://launchpad.support.sap.com/#/notes/3282663, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1160
Affected Version(s): 7.50					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to lack of proper input validation, BSP application (CRM_BSP_FRAME) - versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, allow malicious inputs from untrusted sources, which can be leveraged by an attacker to execute a Reflected Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to hijack a user session, read and modify some sensitive information.	https://launchpad.support.sap.com/#/notes/3282663, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24529		
Affected Version(s): 7.52					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to lack of proper input validation, BSP application (CRM_BSP_FRAME) - versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, allow malicious inputs from untrusted sources, which can be leveraged by an attacker to execute a Reflected Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to hijack a user session, read and modify some sensitive information. **CVE ID : CVE-2023-24529**	https://launchpad.support.sap.com/#/notes/3282663, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1162
Affected Version(s): 700					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (BSP Framework) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the	https://launchpad.support.sap.com/#/notes/3269151, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality and the integrity of the application. **CVE ID : CVE-2023-24521**		
Affected Version(s): 701					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (BSP Framework) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24521**	https://launchpad.support.sap.com/#/notes/3269151, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1164
Affected Version(s): 702					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (BSP Framework) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network	https://launchpad.support.sap.com/#/notes/3269151, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24521**		
Affected Version(s): 731					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (BSP Framework) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24521**	https://launchpad.support.sap.com/#/notes/3269151, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1166
Affected Version(s): 740					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (BSP Framework) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an unauthenticated user to	https://launchpad.support.sap.com/#/notes/3269151, https://www.sap.com/documents/2022/02/fa8	A-SAP-NETW-270223/1167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24521**	65ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 750					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (BSP Framework) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24521**	https://launchpad.support.sap.com/#/notes/3269151, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1168
Affected Version(s): 751					
Improper Neutralization of Input During	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (BSP Framework) - versions 700, 701, 702,	https://launchpad.support.sap.com/#/notes/3269151,	A-SAP-NETW-270223/1169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24521**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 752					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (BSP Framework) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24521**	https://launchpad.support.sap.com/#/notes/3269151, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1170
Affected Version(s): 753					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (BSP Framework) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24521**	https://launchpad.support.sap.com/#/notes/3269151, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1171
Affected Version(s): 754					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (BSP Framework) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application.	https://launchpad.support.sap.com/#/notes/3269151, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24521		
Affected Version(s): 755					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (BSP Framework) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24521**	https://launchpad.support.sap.com/#/notes/3269151, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1173
Affected Version(s): 756					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (BSP Framework) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited	https://launchpad.support.sap.com/#/notes/3269151, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24521**		
Affected Version(s): 757					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (BSP Framework) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application. **CVE ID : CVE-2023-24521**	https://launchpad.support.sap.com/#/notes/3269151, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1175
Affected Version(s): 7.51					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to lack of proper input validation, BSP application (CRM_BSP_FRAME) - versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, allow malicious inputs from untrusted sources, which can be leveraged by an attacker to	https://launchpad.support.sap.com/#/notes/3282663, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-NETW-270223/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute a Reflected Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to hijack a user session, read and modify some sensitive information. **CVE ID : CVE-2023-24529**	c68f7e60039b.html	
Affected Version(s): 75c					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to lack of proper input validation, BSP application (CRM_BSP_FRAME) - versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, allow malicious inputs from untrusted sources, which can be leveraged by an attacker to execute a Reflected Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to hijack a user session, read and modify some sensitive information. **CVE ID : CVE-2023-24529**	https://launchpad.support.sap.com/#/notes/3282663, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1177
Affected Version(s): 75d					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to lack of proper input validation, BSP application (CRM_BSP_FRAME) - versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, allow malicious inputs from untrusted sources,	https://launchpad.support.sap.com/#/notes/3282663, https://www.sap.com/documents/2022/02/fa865ea4-167e-	A-SAP-NETW-270223/1178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which can be leveraged by an attacker to execute a Reflected Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to hijack a user session, read and modify some sensitive information. **CVE ID : CVE-2023-24529**	0010-bca6-c68f7e60039b.html	
Affected Version(s): 75e					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to lack of proper input validation, BSP application (CRM_BSP_FRAME) - versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, allow malicious inputs from untrusted sources, which can be leveraged by an attacker to execute a Reflected Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to hijack a user session, read and modify some sensitive information. **CVE ID : CVE-2023-24529**	https://launchpad.support.sap.com/#/notes/3282663, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1179
Affected Version(s): 75f					
Improper Neutralization of Input During Web Page Generation	14-Feb-2023	6.1	Due to lack of proper input validation, BSP application (CRM_BSP_FRAME) - versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, allow	https://launchpad.support.sap.com/#/notes/3282663, https://www.sap.com/documents/2	A-SAP-NETW-270223/1180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			malicious inputs from untrusted sources, which can be leveraged by an attacker to execute a Reflected Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to hijack a user session, read and modify some sensitive information. **CVE ID : CVE-2023-24529**	022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 75g					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	Due to lack of proper input validation, BSP application (CRM_BSP_FRAME) - versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, allow malicious inputs from untrusted sources, which can be leveraged by an attacker to execute a Reflected Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to hijack a user session, read and modify some sensitive information. **CVE ID : CVE-2023-24529**	https://launchpad.support.sap.com/#/notes/3282663, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-270223/1181
Affected Version(s): 75h					
Improper Neutralization of Input During Web Page	14-Feb-2023	6.1	Due to lack of proper input validation, BSP application (CRM_BSP_FRAME) - versions 700, 701, 702, 731, 740, 750, 751, 752,	https://launchpad.support.sap.com/#/notes/3282663, https://ww	A-SAP-NETW-270223/1182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			75C, 75D, 75E, 75F, 75G, 75H, allow malicious inputs from untrusted sources, which can be leveraged by an attacker to execute a Reflected Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to hijack a user session, read and modify some sensitive information. **CVE ID : CVE-2023-24529**	w.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Product: s4fnd					
Affected Version(s): 1.02					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	SAP CRM WebClient UI - versions WEBCUIF 748, 800, 801, S4FND 102, 103, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an authenticated attacker can cause limited impact on confidentiality of the application. **CVE ID : CVE-2023-24525**	https://launchpad.support.sap.com/#/notes/2788178, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-S4FN-270223/1183
Affected Version(s): 1.03					
Improper Neutralization of Input During Web Page Generation	14-Feb-2023	5.4	SAP CRM WebClient UI - versions WEBCUIF 748, 800, 801, S4FND 102, 103, does not sufficiently encode user-controlled inputs, resulting in Cross-Site	https://launchpad.support.sap.com/#/notes/2788178, https://www.sap.com/d	A-SAP-S4FN-270223/1184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Scripting (XSS) vulnerability. On successful exploitation an authenticated attacker can cause limited impact on confidentiality of the application. **CVE ID : CVE-2023-24525**	ocuments/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Product: solution_manager					
Affected Version(s): 720					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	SAP Solution Manager (System Monitoring) - version 720, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2023-23852**	https://launchpad.support.sap.com/#/notes/3266751, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SOLU-270223/1185
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	SAP Solution Manager (BSP Application) - version 720, allows an authenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can be used to read or modify some sensitive information or craft a payload which may restrict access to the desired resources, resulting in Cross-Site Scripting vulnerability. **CVE ID : CVE-2023-0024**	https://launchpad.support.sap.com/#/notes/3265846, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SOLU-270223/1186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.4	SAP Solution Manager (BSP Application) - version 720, allows an authenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can be used to read or modify some sensitive information or craft a payload which may restrict access to the desired resources. **CVE ID : CVE-2023-0025**	https://launchpad.support.sap.com/#/notes/3267442, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SOLU-270223/1187
URL Redirection to Untrusted Site ('Open Redirect')	14-Feb-2023	5.4	SAP Solution Manager - version 720, allows an authenticated attacker to redirect users to a malicious site due to insufficient URL validation. A successful attack could lead an attacker to read or modify the information or expose the user to a phishing attack. As a result, it has a low impact to confidentiality, integrity and availability. **CVE ID : CVE-2023-23855**	https://launchpad.support.sap.com/#/notes/3270509, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SOLU-270223/1188
Product: s\/4hana					
Affected Version(s): 104					
Missing Authorization	14-Feb-2023	6.5	SAP S/4 HANA Map Treasury Correspondence Format Data does not perform necessary authorization check for an authenticated user,	https://launchpad.support.sap.com/#/notes/2985905, https://www.sap.com/d	A-SAP-S\/4-270223/1189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in escalation of privileges. This could allow an attacker to delete the data with a high impact to availability. **CVE ID : CVE-2023-24524**	ocuments/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 105					
Missing Authorization	14-Feb-2023	6.5	SAP S/4 HANA Map Treasury Correspondence Format Data does not perform necessary authorization check for an authenticated user, resulting in escalation of privileges. This could allow an attacker to delete the data with a high impact to availability. **CVE ID : CVE-2023-24524**	https://launchpad.support.sap.com/#/notes/2985905, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-S\/4-270223/1190
Vendor: selfwealth					
Product: selfwealth					
Affected Version(s): 3.3.1					
N/A	01-Feb-2023	7.5	Selfwealth iOS mobile App 3.3.1 is vulnerable to Insecure App Transport Security (ATS) Settings. **CVE ID : CVE-2023-23131**	N/A	A-SEL-SELF-270223/1191
Use of Hard-coded Credentials	01-Feb-2023	7.5	Selfwealth iOS mobile App 3.3.1 is vulnerable to Sensitive key disclosure. The application reveals hardcoded API keys.	N/A	A-SEL-SELF-270223/1192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23132		
Vendor: send_pdf_for_contact_form_7_project					
Product: send_pdf_for_contact_form_7					
Affected Version(s): * Up to (excluding) 0.9.9.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The Send PDF for Contact Form 7 WordPress plugin before 0.9.9.2 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins. **CVE ID : CVE-2023-0143**	N/A	A-SEN-SEND-270223/1193
Vendor: shapedplugin					
Product: location_weather					
Affected Version(s): * Up to (excluding) 1.3.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	The Location Weather WordPress plugin before 1.3.4 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	N/A	A-SHA-LOCA-270223/1194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0360		
Product: wp_tabs					
Affected Version(s): * Up to (excluding) 2.1.15					
Cross-Site Request Forgery (CSRF)	14-Feb-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in ShapedPlugin WP Tabs – Responsive Tabs Plugin for WordPress plugin <= 2.1.14 versions. **CVE ID : CVE-2023-25065**	N/A	A-SHA-WP_T-270223/1195
Vendor: Shopex					
Product: ecshop					
Affected Version(s): 4.1.5					
Unrestricted Upload of File with Dangerous Type	11-Feb-2023	9.8	A vulnerability was found in EcShop 4.1.5. It has been classified as critical. This affects an unknown part of the file /ecshop/admin/template.php of the component PHP File Handler. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-220641 was assigned to this vulnerability. **CVE ID : CVE-2023-0783**	N/A	A-SHO-ECSH-270223/1196
Vendor: Shopware					
Product: swagpaypal					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 5.4.4					
N/A	03-Feb-2023	7.5	SwagPayPal is a PayPal integration for shopware/platform. If JavaScript-based PayPal checkout methods are used (PayPal Plus, Smart Payment Buttons, SEPA, Pay Later, Venmo, Credit card), the amount and item list sent to PayPal may not be identical to the one in the created order. The problem has been fixed with version 5.4.4. As a workaround, disable the aforementioned payment methods or use the Security Plugin in version >= 1.0.21. **CVE ID : CVE-2023-23941**	https://github.com/shopware/SwagPayPal/commit/57db5f4a57ef0a1646b509b415de9f03bf441b08	A-SHO-SWAG-270223/1197
Vendor: shortpixel					
Product: enable_media_replace					
Affected Version(s): * Up to (excluding) 4.0.2					
Unrestricted Upload of File with Dangerous Type	13-Feb-2023	8.8	The Enable Media Replace WordPress plugin before 4.0.2 does not prevent authors from uploading arbitrary files to the site, which may allow them to upload PHP shells on affected sites. **CVE ID : CVE-2023-0255**	N/A	A-SHO-ENAB-270223/1198
Vendor: Siemens					
Product: comos					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 10.2 Up to (excluding) 10.3.3.1.45					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-Feb-2023	9.8	A vulnerability has been identified in COMOS V10.2 (All versions), COMOS V10.3.3.1 (All versions < V10.3.3.1.45), COMOS V10.3.3.2 (All versions < V10.3.3.2.33), COMOS V10.3.3.3 (All versions < V10.3.3.3.9), COMOS V10.3.3.4 (All versions < V10.3.3.4.6), COMOS V10.4.0.0 (All versions < V10.4.0.0.31), COMOS V10.4.1.0 (All versions < V10.4.1.0.32), COMOS V10.4.2.0 (All versions < V10.4.2.0.25). Cache validation service in COMOS is vulnerable to Structured Exception Handler (SEH) based buffer overflow. This could allow an attacker to execute arbitrary code on the target system or cause denial of service condition. **CVE ID : CVE-2023-24482**	https://cert-portal.siemens.com/productcert/pdf/ssa-693110.pdf	A-SIE-COMO-270223/1199
Affected Version(s): From (including) 10.3.3.2 Up to (excluding) 10.3.3.2.33					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-Feb-2023	9.8	A vulnerability has been identified in COMOS V10.2 (All versions), COMOS V10.3.3.1 (All versions < V10.3.3.1.45), COMOS V10.3.3.2 (All versions < V10.3.3.2.33), COMOS V10.3.3.3 (All versions < V10.3.3.3.9), COMOS V10.3.3.4 (All versions	https://cert-portal.siemens.com/productcert/pdf/ssa-693110.pdf	A-SIE-COMO-270223/1200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V10.3.3.4.6), COMOS V10.4.0.0 (All versions < V10.4.0.0.31), COMOS V10.4.1.0 (All versions < V10.4.1.0.32), COMOS V10.4.2.0 (All versions < V10.4.2.0.25). Cache validation service in COMOS is vulnerable to Structured Exception Handler (SEH) based buffer overflow. This could allow an attacker to execute arbitrary code on the target system or cause denial of service condition. **CVE ID : CVE-2023-24482**		
Affected Version(s): From (including) 10.3.3.3 Up to (excluding) 10.3.3.3.9					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-Feb-2023	9.8	A vulnerability has been identified in COMOS V10.2 (All versions), COMOS V10.3.3.1 (All versions < V10.3.3.1.45), COMOS V10.3.3.2 (All versions < V10.3.3.2.33), COMOS V10.3.3.3 (All versions < V10.3.3.3.9), COMOS V10.3.3.4 (All versions < V10.3.3.4.6), COMOS V10.4.0.0 (All versions < V10.4.0.0.31), COMOS V10.4.1.0 (All versions < V10.4.1.0.32), COMOS V10.4.2.0 (All versions < V10.4.2.0.25). Cache validation service in COMOS is vulnerable to Structured Exception Handler (SEH) based buffer overflow. This	https://cert-portal.siemens.com/productcert/pdf/ssa-693110.pdf	A-SIE-COMO-270223/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker to execute arbitrary code on the target system or cause denial of service condition. **CVE ID : CVE-2023-24482**		
Affected Version(s): From (including) 10.3.3.4 Up to (excluding) 10.3.3.4.6					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-Feb-2023	9.8	A vulnerability has been identified in COMOS V10.2 (All versions), COMOS V10.3.3.1 (All versions < V10.3.3.1.45), COMOS V10.3.3.2 (All versions < V10.3.3.2.33), COMOS V10.3.3.3 (All versions < V10.3.3.3.9), COMOS V10.3.3.4 (All versions < V10.3.3.4.6), COMOS V10.4.0.0 (All versions < V10.4.0.0.31), COMOS V10.4.1.0 (All versions < V10.4.1.0.32), COMOS V10.4.2.0 (All versions < V10.4.2.0.25). Cache validation service in COMOS is vulnerable to Structured Exception Handler (SEH) based buffer overflow. This could allow an attacker to execute arbitrary code on the target system or cause denial of service condition. **CVE ID : CVE-2023-24482**	https://cert-portal.siemens.com/productcert/pdf/ssa-693110.pdf	A-SIE-COMO-270223/1202
Affected Version(s): From (including) 10.4.0.0 Up to (excluding) 10.4.0.0.31					
Buffer Copy without	14-Feb-2023	9.8	A vulnerability has been identified in COMOS V10.2 (All	https://cert-portal.siemens.com/prod	A-SIE-COMO-270223/1203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			versions), COMOS V10.3.3.1 (All versions < V10.3.3.1.45), COMOS V10.3.3.2 (All versions < V10.3.3.2.33), COMOS V10.3.3.3 (All versions < V10.3.3.3.9), COMOS V10.3.3.4 (All versions < V10.3.3.4.6), COMOS V10.4.0.0 (All versions < V10.4.0.0.31), COMOS V10.4.1.0 (All versions < V10.4.1.0.32), COMOS V10.4.2.0 (All versions < V10.4.2.0.25). Cache validation service in COMOS is vulnerable to Structured Exception Handler (SEH) based buffer overflow. This could allow an attacker to execute arbitrary code on the target system or cause denial of service condition. **CVE ID : CVE-2023-24482**	uctcert/pdf/ssa-693110.pdf	
Affected Version(s): From (including) 10.4.1.0 Up to (excluding) 10.4.1.0.32					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-Feb-2023	9.8	A vulnerability has been identified in COMOS V10.2 (All versions), COMOS V10.3.3.1 (All versions < V10.3.3.1.45), COMOS V10.3.3.2 (All versions < V10.3.3.2.33), COMOS V10.3.3.3 (All versions < V10.3.3.3.9), COMOS V10.3.3.4 (All versions < V10.3.3.4.6), COMOS V10.4.0.0 (All versions < V10.4.0.0.31), COMOS V10.4.1.0 (All versions	https://cert-portal.siemens.com/productcert/pdf/ssa-693110.pdf	A-SIE-COMO-270223/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V10.4.1.0.32), COMOS V10.4.2.0 (All versions < V10.4.2.0.25). Cache validation service in COMOS is vulnerable to Structured Exception Handler (SEH) based buffer overflow. This could allow an attacker to execute arbitrary code on the target system or cause denial of service condition. **CVE ID : CVE-2023-24482**		
Affected Version(s): From (including) 10.4.2.0 Up to (excluding) 10.4.2.0.25					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-Feb-2023	9.8	A vulnerability has been identified in COMOS V10.2 (All versions), COMOS V10.3.3.1 (All versions < V10.3.3.1.45), COMOS V10.3.3.2 (All versions < V10.3.3.2.33), COMOS V10.3.3.3 (All versions < V10.3.3.3.9), COMOS V10.3.3.4 (All versions < V10.3.3.4.6), COMOS V10.4.0.0 (All versions < V10.4.0.0.31), COMOS V10.4.1.0 (All versions < V10.4.1.0.32), COMOS V10.4.2.0 (All versions < V10.4.2.0.25). Cache validation service in COMOS is vulnerable to Structured Exception Handler (SEH) based buffer overflow. This could allow an attacker to execute arbitrary code on the target	https://cert-portal.siemens.com/productcert/pdf/ssa-693110.pdf	A-SIE-COMO-270223/1205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system or cause denial of service condition. **CVE ID : CVE-2023-24482**		
Product: parasolid					
Affected Version(s): From (including) 34.0 Up to (excluding) 34.0.254					
Out-of-bounds Read	14-Feb-2023	7.8	A vulnerability has been identified in Parasolid V34.0 (All versions < V34.0.254), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.170), Parasolid V35.1 (All versions < V35.1.150), Solid Edge SE2022 (All versions < V2210Update12). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-25140**	https://cert-portal.siemens.com/productcert/pdf/ssa-836777.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-PARA-270223/1206
Affected Version(s): From (including) 34.1 Up to (excluding) 34.1.242					
Out-of-bounds Read	14-Feb-2023	7.8	A vulnerability has been identified in Parasolid V34.0 (All versions < V34.0.254), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.170), Parasolid V35.1 (All versions < V35.1.150),	https://cert-portal.siemens.com/productcert/pdf/ssa-836777.pdf, https://cert-portal.siemens.com/productcert/pdf/	A-SIE-PARA-270223/1207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Solid Edge SE2022 (All versions < V2210Update12). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-25140**	ssa-491245.pdf	
Affected Version(s): From (including) 35.0 Up to (excluding) 35.0.170					
Out-of-bounds Read	14-Feb-2023	7.8	A vulnerability has been identified in Parasolid V34.0 (All versions < V34.0.254), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.170), Parasolid V35.1 (All versions < V35.1.150), Solid Edge SE2022 (All versions < V2210Update12). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-25140**	https://cert-portal.siemens.com/productcert/pdf/ssa-836777.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-PARA-270223/1208
Affected Version(s): From (including) 35.1 Up to (excluding) 35.1.150					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	14-Feb-2023	7.8	A vulnerability has been identified in Parasolid V34.0 (All versions < V34.0.254), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.170), Parasolid V35.1 (All versions < V35.1.150), Solid Edge SE2022 (All versions < V2210Update12). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-25140**	https://cert-portal.siemens.com/productcert/pdf/ssa-836777.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-PARA-270223/1209
Product: solid_edge					
Affected Version(s): se2022					
Out-of-bounds Read	14-Feb-2023	7.8	A vulnerability has been identified in Parasolid V34.0 (All versions < V34.0.254), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.170), Parasolid V35.1 (All versions < V35.1.150), Solid Edge SE2022 (All versions < V2210Update12). The affected applications contain an out of bounds read past the	https://cert-portal.siemens.com/productcert/pdf/ssa-836777.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-25140**		
Product: solid_edge_se2023					
Affected Version(s): * Up to (excluding) 2210.0002.004					
Stack-based Buffer Overflow	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2023 (All versions < V2023Update2). The affected application is vulnerable to stack-based buffer while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-24549**	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1211
Heap-based Buffer Overflow	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2023 (All versions < V2023Update2). The affected application is vulnerable to heap-based buffer while	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-24550**		
Heap-based Buffer Overflow	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2023 (All versions < V2023Update2). The affected application is vulnerable to heap-based buffer underflow while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-24551**	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1213
Out-of-bounds Read	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2023 (All versions < V2023Update2). The affected application contains an out of bounds read past the end of an allocated buffer while parsing a specially crafted PAR	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file. This could allow an attacker to to execute code in the context of the current process. **CVE ID : CVE-2023-24552**		
Out-of-bounds Read	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2023 (All versions < V2023Update2). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-24553**	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1215
Out-of-bounds Read	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2023 (All versions < V2023Update2). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the current process. **CVE ID : CVE-2023-24554**		
Out-of-bounds Read	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2023 (All versions < V2023Update2). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-24555**	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1217
Out-of-bounds Read	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2023 (All versions < V2023Update2). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24556		
Out-of-bounds Read	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2023 (All versions < V2023Update2). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-24557**	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1219
Out-of-bounds Read	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2023 (All versions < V2023Update2). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-24558**	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2023 (All versions < V2023Update2). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-24559**	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1221
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2023 (All versions < V2023Update2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an attacker to to execute code in the context of the current process. **CVE ID : CVE-2023-24560**	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2023 (All versions < V2023Update2). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-24561**	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1223
Access of Uninitialized Pointer	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2023 (All versions < V2023Update2). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-24562**	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2023 (All versions < V2023Update2). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-24563**	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1225
Improper Restriction of Operations within the Bounds of a Memory Buffer	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2022 (All versions), Solid Edge SE2023 (All versions < V2023Update2). The affected application contains a memory corruption vulnerability while parsing specially crafted DWG files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19069) **CVE ID : CVE-2023-24564**	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2022 (All versions), Solid Edge SE2023 (All versions < V2023Update2). The affected application is vulnerable to stack-based buffer while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19472) **CVE ID : CVE-2023-24566**	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1227
Use After Free	14-Feb-2023	7.8	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2022 (All versions), Solid Edge SE2023 (All versions < V2023Update2). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted STP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19425)	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24581		
Out-of-bounds Read	14-Feb-2023	5.5	A vulnerability has been identified in Solid Edge SE2022 (All versions < V2210Update12), Solid Edge SE2022 (All versions), Solid Edge SE2023 (All versions < V2023Update2). The affected application contains an out of bounds read past the end of an allocated buffer while parsing a specially crafted STL file. This vulnerability could allow an attacker to disclose sensitive information. (ZDI-CAN-19428) **CVE ID : CVE-2023-24565**	https://cert-portal.siemens.com/productcert/pdf/ssa-491245.pdf	A-SIE-SOLI-270223/1229
Product: tecnomatix_plant_simulation					
Affected Version(s): * Up to (excluding) 2201.0006					
Access of Uninitialized Pointer	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted SPP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19788)	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24978		
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19789) **CVE ID : CVE-2023-24979**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1231
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19790) **CVE ID : CVE-2023-24980**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1232
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions	https://cert-portal.siemens.com/productcert/pdf/	A-SIE-TECN-270223/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19791) **CVE ID : CVE-2023-24981**	ssa-847261.pdf	
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19804) **CVE ID : CVE-2023-24982**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1234
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19805) **CVE ID : CVE-2023-24983**		
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19806) **CVE ID : CVE-2023-24984**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1236
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19807)	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24985		
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19808) **CVE ID : CVE-2023-24986**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1238
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19809) **CVE ID : CVE-2023-24987**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1239
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions	https://cert-portal.siemens.com/productcert/pdf/	A-SIE-TECN-270223/1240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19810) **CVE ID : CVE-2023-24988**	ssa-847261.pdf	
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19811) **CVE ID : CVE-2023-24989**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1241
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19812) **CVE ID : CVE-2023-24990**		
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19813) **CVE ID : CVE-2023-24991**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1243
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19814)	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24992		
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19815) **CVE ID : CVE-2023-24993**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1245
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19816) **CVE ID : CVE-2023-24994**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1246
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions	https://cert-portal.siemens.com/productcert/pdf/	A-SIE-TECN-270223/1247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19817) **CVE ID : CVE-2023-24995**	ssa-847261.pdf	
Out-of-bounds Write	14-Feb-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19818) **CVE ID : CVE-2023-24996**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-270223/1248
Vendor: simple_sales_management_system_project					
Product: simple_sales_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation	07-Feb-2023	6.1	Cross site scripting (XSS) vulnerability in sourcecodester oretnom23 sales management system 1.0, allows attackers to execute arbitrary code	N/A	A-SIM-SIMP-270223/1249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			via the product_name and product_price inputs in file print.php. **CVE ID : CVE-2023-23026**		
Vendor: siteground					
Product: siteground_security					
Affected Version(s): * Up to (excluding) 1.3.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Feb-2023	8.8	The SiteGround Security WordPress plugin before 1.3.1 does not properly sanitize user input before using it in an SQL query, leading to an authenticated SQL injection issue. **CVE ID : CVE-2023-0234**	N/A	A-SIT-SITE-270223/1250
Vendor: slims_project					
Product: slims					
Affected Version(s): 9.5.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	6.1	SLIMS v9.5.2 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /customs/loan_by_class.php?reportView. **CVE ID : CVE-2023-24086**	N/A	A-SLI-SLIM-270223/1251
Vendor: smartwp					
Product: lightweight_accordion					
Affected Version(s): * Up to (excluding) 1.5.15					
Improper Neutralization of Input	13-Feb-2023	5.4	The Lightweight Accordion WordPress plugin before 1.5.15 does not validate and	N/A	A-SMA-LIGH-270223/1252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0373**		
Vendor: Solarwinds					
Product: orion_platform					
Affected Version(s): 2022.4.1					
Deserialization of Untrusted Data	15-Feb-2023	7.2	SolarWinds Platform version 2022.4.1 was found to be susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to the SolarWinds Web Console to execute arbitrary commands. **CVE ID : CVE-2023-23836**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2023-23836	A-SOL-ORIO-270223/1253
Vendor: Sonicwall					
Product: email_security					
Affected Version(s): * Up to (including) 10.0.19.7431					
Generation of Error Message Containing Sensitive Information	14-Feb-2023	5.3	SonicWall Email Security contains a vulnerability that could permit a remote unauthenticated attacker access to an error page that includes sensitive information	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0002	A-SON-EMAI-270223/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			about users email addresses. **CVE ID : CVE-2023-0655**		
Vendor: Southrivertech					
Product: titan_ftp_server					
Affected Version(s): * Up to (including) 1.94.1205					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Feb-2023	8.8	An issue was discovered in TitanFTP through 1.94.1205. The move-file function has a path traversal vulnerability in the newPath parameter. An authenticated attacker can upload any file and then move it anywhere on the server's filesystem. **CVE ID : CVE-2023-22629**	N/A	A-SOU-TITA-270223/1255
Vendor: Splunk					
Product: add-on_builder					
Affected Version(s): From (including) 4.1.0 Up to (excluding) 4.1.2					
Improper Certificate Validation	14-Feb-2023	5.3	In Splunk Add-on Builder (AoB) versions below 4.1.2 and the Splunk CloudConnect SDK versions below 3.1.3, requests to third-party APIs through the REST API Modular Input incorrectly revert to using HTTP to connect after a failure to connect over HTTPS occurs. The vulnerability affects AoB and apps that AoB generates when using the REST API Modular	https://advisory.splunk.com/advisories/SVD-2023-0213	A-SPL-ADD--270223/1256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Input functionality through its user interface. The vulnerability also potentially affects third-party apps and add-ons that call the *cloudconnectlib.splunktacollectorlib.cloud_connect_mod_input* Python class directly. **CVE ID : CVE-2023-22943**		
Product: cloudconnect_software_development_kit					
Affected Version(s): From (including) 3.1.0 Up to (excluding) 3.1.3					
Improper Certificate Validation	14-Feb-2023	5.3	In Splunk Add-on Builder (AoB) versions below 4.1.2 and the Splunk CloudConnect SDK versions below 3.1.3, requests to third-party APIs through the REST API Modular Input incorrectly revert to using HTTP to connect after a failure to connect over HTTPS occurs. The vulnerability affects AoB and apps that AoB generates when using the REST API Modular Input functionality through its user interface. The vulnerability also potentially affects third-party apps and add-ons that call the *cloudconnectlib.splunktacollectorlib.cloud_co	https://advisory.splunk.com/advisories/SVD-2023-0213	A-SPL-CLOU-270223/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nnect_mod_input* Python class directly. **CVE ID : CVE-2023-22943**		
Product: splunk					
Affected Version(s): From (including) 8.1.0 Up to (excluding) 8.1.13					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	14-Feb-2023	8.8	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'display.page.search.patterns.sensitivity' search parameter lets a search bypass [SPL safeguards for risky commands](https://docs.splunk.com/Documentation/Splunk/latest/Security/SPLsafeguards). The vulnerability requires a higher privileged user to initiate a request within their browser and only affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22935**	https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0205	A-SPL-SPLU-270223/1258
N/A	14-Feb-2023	8.8	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'map' search processing language (SPL) command lets a search [bypass SPL safeguards for risky commands](https://docs.splunk.com/Documentation/Splunk/latest/Security/SPLsafeguards). The vulnerability requires a higher privileged user to	https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0209	A-SPL-SPLU-270223/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiate a request within their browser and only affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22939**		
N/A	14-Feb-2023	8	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'pivot' search processing language (SPL) command lets a search bypass [SPL safeguards for risky commands](https://docs.splunk.com/Documentation/Splunk/latest/Security/SPLsafeguards) using a saved search job. The vulnerability requires an authenticated user to craft the saved job and a higher privileged user to initiate a request within their browser. The vulnerability affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22934**	https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0204	A-SPL-SPLU-270223/1260
N/A	14-Feb-2023	7.5	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, an improperly-formatted 'INGEST_EVAL' parameter in a [Field Transformation](https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Managefieldtransforms)	https://advisory.splunk.com/advisories/SVD-2023-0211, https://research.splunk.com/application/08978eca-caff-44c1-84dc-	A-SPL-SPLU-270223/1261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crashes the Splunk daemon (splunkd). **CVE ID : CVE-2023-22941**	53f17def4e14/	
Server-Side Request Forgery (SSRF)	14-Feb-2023	6.3	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'search_listener' parameter in a search allows for a blind server-side request forgery (SSRF) by an authenticated user. The initiator of the request cannot see the response without the presence of an additional vulnerability within the environment. **CVE ID : CVE-2023-22936**	https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0206	A-SPL-SPLU-270223/1262
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, a View allows for Cross-Site Scripting (XSS) in an extensible mark-up language (XML) View through the 'layoutPanel' attribute in the 'module' tag'. The vulnerability affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22933**	https://research.splunk.com/application/9ac2bfea-a234-4a18-9d37-6d747e85c2e4, https://advisory.splunk.com/advisories/SVD-2023-0203	A-SPL-SPLU-270223/1263
N/A	14-Feb-2023	5.7	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, aliases of the 'collect' search processing language (SPL) command,	https://advisory.splunk.com/advisories/SVD-2023-0210	A-SPL-SPLU-270223/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including 'summaryindex', 'sumindex', 'stash',' mcollect', and 'meventcollect', were not designated as safeguarded commands. The commands could potentially allow for the exposing of data to a summary index that unprivileged users could access. The vulnerability requires a higher privileged user to initiate a request within their browser, and only affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22940**		
Incorrect Default Permissions	14-Feb-2023	4.3	In Splunk Enterprise versions below 8.1.13 and 8.2.10, the 'createrss' external search command overwrites existing Resource Description Format Site Summary (RSS) feeds without verifying permissions. This feature has been deprecated and disabled by default. **CVE ID : CVE-2023-22931**	https://advisory.splunk.com/advisories/SVD-2023-0201, https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd/	A-SPL-SPLU-270223/1265
Unrestricted Upload of File with	14-Feb-2023	4.3	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the lookup table upload feature let a user	https://advisory.splunk.com/advisor	A-SPL-SPLU-270223/1266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			upload lookup tables with unnecessary filename extensions. Lookup table file extensions may now be one of the following only: .csv, .csv.gz, .kmz, .kml, .mmdb, or .mmdb.gzl. For more information on lookup table files, see [About lookups](https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Aboutlookupsandfieldactions). **CVE ID : CVE-2023-22937**	ies/SVD-2023-0207	
N/A	14-Feb-2023	4.3	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'sendemail' REST API endpoint lets any authenticated user send an email as the Splunk instance. The endpoint is now restricted to the 'splunk-system-user' account on the local instance. **CVE ID : CVE-2023-22938**	https://advisory.splunk.com/advisories/SVD-2023-0208	A-SPL-SPLU-270223/1267
Cross-Site Request Forgery (CSRF)	14-Feb-2023	4.3	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, a cross-site request forgery in the Splunk Secure Gateway (SSG) app in the 'kvstore_client' REST endpoint lets a potential attacker update SSG [App Key	https://research.splunk.com/application/4742d5f7-ce00-45ce-9c79-5e98b43b4410/, https://advisory.splunk.com/advisor	A-SPL-SPLU-270223/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Value Store (KV store)](https://docs.splunk.com/Documentation/Splunk/latest/Admin/AboutKVstore) collections using an HTTP GET request. SSG is a Splunk-built app that comes with Splunk Enterprise. The vulnerability affects instances with SSG and Splunk Web enabled. **CVE ID : CVE-2023-22942**	ies/SVD-2023-0212	
Affected Version(s): From (including) 8.2.0 Up to (excluding) 8.2.10					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	14-Feb-2023	8.8	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'display.page.search.patterns.sensitivity' search parameter lets a search bypass [SPL safeguards for risky commands](https://docs.splunk.com/Documentation/Splunk/latest/Security/SPLsafeguards). The vulnerability requires a higher privileged user to initiate a request within their browser and only affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22935**	https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0205	A-SPL-SPLU-270223/1269
N/A	14-Feb-2023	8.8	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'map' search processing language (SPL)	https://research.splunk.com/application/ee69374a-d27e-	A-SPL-SPLU-270223/1270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command lets a search [bypass SPL safeguards for risky commands](https://docs.splunk.com/Documentation/Splunk/latest/Security/SPLsafeguards). The vulnerability requires a higher privileged user to initiate a request within their browser and only affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22939**	4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0209	
N/A	14-Feb-2023	8	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'pivot' search processing language (SPL) command lets a search bypass [SPL safeguards for risky commands](https://docs.splunk.com/Documentation/Splunk/latest/Security/SPLsafeguards) using a saved search job. The vulnerability requires an authenticated user to craft the saved job and a higher privileged user to initiate a request within their browser. The vulnerability affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22934**	https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0204	A-SPL-SPLU-270223/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.5	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, an improperly-formatted 'INGEST_EVAL' parameter in a [Field Transformation](https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Managefieldtransforms) crashes the Splunk daemon (splunkd). **CVE ID : CVE-2023-22941**	https://advisory.splunk.com/advisories/SVD-2023-0211, https://research.splunk.com/application/08978eca-caff-44c1-84dc-53f17def4e14/	A-SPL-SPLU-270223/1272
Server-Side Request Forgery (SSRF)	14-Feb-2023	6.3	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'search_listener' parameter in a search allows for a blind server-side request forgery (SSRF) by an authenticated user. The initiator of the request cannot see the response without the presence of an additional vulnerability within the environment. **CVE ID : CVE-2023-22936**	https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0206	A-SPL-SPLU-270223/1273
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, a View allows for Cross-Site Scripting (XSS) in an extensible mark-up language (XML) View through the 'layoutPanel' attribute in the 'module' tag'. The vulnerability affects	https://research.splunk.com/application/9ac2bfea-a234-4a18-9d37-6d747e85c2e4, https://advisory.splunk.com/advisor	A-SPL-SPLU-270223/1274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			instances with Splunk Web enabled. **CVE ID : CVE-2023-22933**	ies/SVD-2023-0203	
N/A	14-Feb-2023	5.7	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, aliases of the 'collect' search processing language (SPL) command, including 'summaryindex', 'sumindex', 'stash',' mcollect', and 'meventcollect', were not designated as safeguarded commands. The commands could potentially allow for the exposing of data to a summary index that unprivileged users could access. The vulnerability requires a higher privileged user to initiate a request within their browser, and only affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22940**	https://advisory.splunk.com/advisories/SVD-2023-0210	A-SPL-SPLU-270223/1275
Incorrect Default Permissions	14-Feb-2023	4.3	In Splunk Enterprise versions below 8.1.13 and 8.2.10, the 'createrss' external search command overwrites existing Resource Description Format Site Summary (RSS) feeds without verifying permissions.	https://advisory.splunk.com/advisories/SVD-2023-0201, https://research.splunk.com/application/ee69374a-d27e-	A-SPL-SPLU-270223/1276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This feature has been deprecated and disabled by default. **CVE ID : CVE-2023-22931**	4136-adac-956a96ff60fd/	
Unrestricted Upload of File with Dangerous Type	14-Feb-2023	4.3	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the lookup table upload feature let a user upload lookup tables with unnecessary filename extensions. Lookup table file extensions may now be one of the following only: .csv, .csv.gz, .kmz, .kml, .mmdb, or .mmdb.gzl. For more information on lookup table files, see [About lookups](https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Aboutlookupsandfieldactions). **CVE ID : CVE-2023-22937**	https://advisory.splunk.com/advisories/SVD-2023-0207	A-SPL-SPLU-270223/1277
N/A	14-Feb-2023	4.3	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'sendemail' REST API endpoint lets any authenticated user send an email as the Splunk instance. The endpoint is now restricted to the 'splunk-system-user' account on the local instance. **CVE ID : CVE-2023-22938**	https://advisory.splunk.com/advisories/SVD-2023-0208	A-SPL-SPLU-270223/1278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	14-Feb-2023	4.3	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, a cross-site request forgery in the Splunk Secure Gateway (SSG) app in the 'kvstore_client' REST endpoint lets a potential attacker update SSG [App Key Value Store (KV store)](https://docs.splunk.com/Documentation/Splunk/latest/Admin/AboutKVstore) collections using an HTTP GET request. SSG is a Splunk-built app that comes with Splunk Enterprise. The vulnerability affects instances with SSG and Splunk Web enabled. **CVE ID : CVE-2023-22942**	https://research.splunk.com/application/4742d5f7-ce00-45ce-9c79-5e98b43b4410/, https://advisory.splunk.com/advisories/SVD-2023-0212	A-SPL-SPLU-270223/1279
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.0.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	14-Feb-2023	8.8	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'display.page.search.patterns.sensitivity' search parameter lets a search bypass [SPL safeguards for risky commands](https://docs.splunk.com/Documentation/Splunk/latest/Security/SPLsafeguards). The vulnerability requires a higher privileged user to initiate a request within	https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0205	A-SPL-SPLU-270223/1280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			their browser and only affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22935**		
N/A	14-Feb-2023	8.8	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'map' search processing language (SPL) command lets a search [bypass SPL safeguards for risky commands](https://docs.splunk.com/Documentation/Splunk/latest/Security/SPLsafeguards). The vulnerability requires a higher privileged user to initiate a request within their browser and only affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22939**	https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0209	A-SPL-SPLU-270223/1281
N/A	14-Feb-2023	8	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'pivot' search processing language (SPL) command lets a search bypass [SPL safeguards for risky commands](https://docs.splunk.com/Documentation/Splunk/latest/Security/SPLsafeguards) using a saved search job. The vulnerability requires an authenticated user to craft the saved job and	https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0204	A-SPL-SPLU-270223/1282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a higher privileged user to initiate a request within their browser. The vulnerability affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22934**		
N/A	14-Feb-2023	7.5	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, an improperly-formatted 'INGEST_EVAL' parameter in a [Field Transformation](https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Managefieldtransforms) crashes the Splunk daemon (splunkd). **CVE ID : CVE-2023-22941**	https://advisory.splunk.com/advisories/SVD-2023-0211, https://research.splunk.com/application/08978eca-caff-44c1-84dc-53f17def4e14/	A-SPL-SPLU-270223/1283
Server-Side Request Forgery (SSRF)	14-Feb-2023	6.3	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'search_listener' parameter in a search allows for a blind server-side request forgery (SSRF) by an authenticated user. The initiator of the request cannot see the response without the presence of an additional vulnerability within the environment. **CVE ID : CVE-2023-22936**	https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0206	A-SPL-SPLU-270223/1284
Improper Neutralizat	14-Feb-2023	6.1	In Splunk Enterprise 9.0 versions before	https://advisory.splunk.	A-SPL-SPLU-270223/1285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			9.0.4, a View allows for Cross-Site Scripting (XSS) through the error message in a Base64-encoded image. The vulnerability affects instances with Splunk Web enabled. It does not affect Splunk Enterprise versions below 9.0. **CVE ID : CVE-2023-22932**	com/advisories/SVD-2023-0202	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, a View allows for Cross-Site Scripting (XSS) in an extensible mark-up language (XML) View through the 'layoutPanel' attribute in the 'module' tag'. The vulnerability affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22933**	https://research.splunk.com/application/9ac2bfea-a234-4a18-9d37-6d747e85c2e4, https://advisory.splunk.com/advisories/SVD-2023-0203	A-SPL-SPLU-270223/1286
N/A	14-Feb-2023	5.7	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, aliases of the 'collect' search processing language (SPL) command, including 'summaryindex', 'sumindex', 'stash',' mcollect', and 'meventcollect', were not designated as safeguarded commands. The commands could	https://advisory.splunk.com/advisories/SVD-2023-0210	A-SPL-SPLU-270223/1287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially allow for the exposing of data to a summary index that unprivileged users could access. The vulnerability requires a higher privileged user to initiate a request within their browser, and only affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22940**		
Unrestricted Upload of File with Dangerous Type	14-Feb-2023	4.3	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the lookup table upload feature let a user upload lookup tables with unnecessary filename extensions. Lookup table file extensions may now be one of the following only: .csv, .csv.gz, .kmz, .kml, .mmdb, or .mmdb.gzl. For more information on lookup table files, see [About lookups](https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Aboutlookupsandfieldactions). **CVE ID : CVE-2023-22937**	https://advisory.splunk.com/advisories/SVD-2023-0207	A-SPL-SPLU-270223/1288
N/A	14-Feb-2023	4.3	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'sendemail' REST API endpoint lets any authenticated user send	https://advisory.splunk.com/advisories/SVD-2023-0208	A-SPL-SPLU-270223/1289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an email as the Splunk instance. The endpoint is now restricted to the 'splunk-system-user' account on the local instance. **CVE ID : CVE-2023-22938**		
Cross-Site Request Forgery (CSRF)	14-Feb-2023	4.3	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, a cross-site request forgery in the Splunk Secure Gateway (SSG) app in the 'kvstore_client' REST endpoint lets a potential attacker update SSG [App Key Value Store (KV store)](https://docs.splunk.com/Documentation/Splunk/latest/Admin/AboutKVstore) collections using an HTTP GET request. SSG is a Splunk-built app that comes with Splunk Enterprise. The vulnerability affects instances with SSG and Splunk Web enabled. **CVE ID : CVE-2023-22942**	https://research.splunk.com/application/4742d5f7-ce00-45ce-9c79-5e98b43b4410/, https://advisory.splunk.com/advisories/SVD-2023-0212	A-SPL-SPLU-270223/1290
Product: splunk_cloud_platform					
Affected Version(s): * Up to (excluding) 8.2.2203					
Incorrect Default Permissions	14-Feb-2023	4.3	In Splunk Enterprise versions below 8.1.13 and 8.2.10, the 'createrss' external search command overwrites existing	https://advisory.splunk.com/advisories/SVD-2023-0201, https://rese	A-SPL-SPLU-270223/1291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Resource Description Format Site Summary (RSS) feeds without verifying permissions. This feature has been deprecated and disabled by default. **CVE ID : CVE-2023-22931**	arch.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd/	
Affected Version(s): * Up to (excluding) 9.0.2209					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, a View allows for Cross-Site Scripting (XSS) in an extensible mark-up language (XML) View through the 'layoutPanel' attribute in the 'module' tag'. The vulnerability affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22933**	https://research.splunk.com/application/9ac2bfea-a234-4a18-9d37-6d747e85c2e4, https://advisory.splunk.com/advisories/SVD-2023-0203	A-SPL-SPLU-270223/1292
Affected Version(s): * Up to (excluding) 9.0.2209.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	14-Feb-2023	8.8	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'display.page.search.patterns.sensitivity' search parameter lets a search bypass [SPL safeguards for risky commands](https://docs.splunk.com/Documentation/Splunk/latest/Security/SPLsafeguards). The vulnerability requires a higher privileged user to initiate a request within	https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0205	A-SPL-SPLU-270223/1293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			their browser and only affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22935**		
N/A	14-Feb-2023	8.8	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'map' search processing language (SPL) command lets a search [bypass SPL safeguards for risky commands](https://docs.splunk.com/Documentation/Splunk/latest/Security/SPLsafeguards). The vulnerability requires a higher privileged user to initiate a request within their browser and only affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22939**	https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0209	A-SPL-SPLU-270223/1294
N/A	14-Feb-2023	8	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'pivot' search processing language (SPL) command lets a search bypass [SPL safeguards for risky commands](https://docs.splunk.com/Documentation/Splunk/latest/Security/SPLsafeguards) using a saved search job. The vulnerability requires an authenticated user to craft the saved job and	https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0204	A-SPL-SPLU-270223/1295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a higher privileged user to initiate a request within their browser. The vulnerability affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22934**		
N/A	14-Feb-2023	7.5	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, an improperly-formatted 'INGEST_EVAL' parameter in a [Field Transformation](https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Managefieldtransforms) crashes the Splunk daemon (splunkd). **CVE ID : CVE-2023-22941**	https://advisory.splunk.com/advisories/SVD-2023-0211, https://research.splunk.com/application/08978eca-caff-44c1-84dc-53f17def4e14/	A-SPL-SPLU-270223/1296
Server-Side Request Forgery (SSRF)	14-Feb-2023	6.3	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'search_listener' parameter in a search allows for a blind server-side request forgery (SSRF) by an authenticated user. The initiator of the request cannot see the response without the presence of an additional vulnerability within the environment. **CVE ID : CVE-2023-22936**	https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd, https://advisory.splunk.com/advisories/SVD-2023-0206	A-SPL-SPLU-270223/1297
Improper Neutralizat	14-Feb-2023	6.1	In Splunk Enterprise 9.0 versions before	https://advisory.splunk.	A-SPL-SPLU-270223/1298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			9.0.4, a View allows for Cross-Site Scripting (XSS) through the error message in a Base64-encoded image. The vulnerability affects instances with Splunk Web enabled. It does not affect Splunk Enterprise versions below 9.0. **CVE ID : CVE-2023-22932**	com/advisories/SVD-2023-0202	
N/A	14-Feb-2023	5.7	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, aliases of the 'collect' search processing language (SPL) command, including 'summaryindex', 'sumindex', 'stash',' mcollect', and 'meventcollect', were not designated as safeguarded commands. The commands could potentially allow for the exposing of data to a summary index that unprivileged users could access. The vulnerability requires a higher privileged user to initiate a request within their browser, and only affects instances with Splunk Web enabled. **CVE ID : CVE-2023-22940**	https://advisory.splunk.com/advisories/SVD-2023-0210	A-SPL-SPLU-270223/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	14-Feb-2023	4.3	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the lookup table upload feature let a user upload lookup tables with unnecessary filename extensions. Lookup table file extensions may now be one of the following only: .csv, .csv.gz, .kmz, .kml, .mmdb, or .mmdb.gzl. For more information on lookup table files, see [About lookups](https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Aboutlookupsandfieldactions). **CVE ID : CVE-2023-22937**	https://advisory.splunk.com/advisories/SVD-2023-0207	A-SPL-SPLU-270223/1300
N/A	14-Feb-2023	4.3	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'sendemail' REST API endpoint lets any authenticated user send an email as the Splunk instance. The endpoint is now restricted to the 'splunk-system-user' account on the local instance. **CVE ID : CVE-2023-22938**	https://advisory.splunk.com/advisories/SVD-2023-0208	A-SPL-SPLU-270223/1301
Vendor: squidex.io					
Product: squidex					
Affected Version(s): * Up to (excluding) 7.4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	02-Feb-2023	6.5	Cross-Site Request Forgery (CSRF) in GitHub repository squidex/squidex prior to 7.4.0. **CVE ID : CVE-2023-0642**	https://github.com/squidex/squidex/commit/2da3c41da82eb945832f22bb70dba567ac6ce969, https://huntr.dev/bounties/3bbdafe6-e152-47bb-88a7-fd031725323d	A-SQU-SQUI-270223/1302
Improper Handling of Additional Special Element	02-Feb-2023	6.1	Improper Handling of Additional Special Element in GitHub repository squidex/squidex prior to 7.4.0. **CVE ID : CVE-2023-0643**	https://huntr.dev/bounties/ea90f8b9-d8fe-4432-9a52-4d663400c52f, https://github.com/squidex/squidex/commit/cf4efc52eab17098474d73ccff6c136fc2f737db	A-SQU-SQUI-270223/1303
Vendor: starliteproject					
Product: starlite					
Affected Version(s): * Up to (excluding) 1.51.2					
Allocation of Resources Without Limits or Throttling	15-Feb-2023	7.5	Starlite is an Asynchronous Server Gateway Interface (ASGI) framework. Prior to version 1.5.2, the request body parsing in `starlite` allows a potentially unauthenticated	https://github.com/starlite-api/starlite/security/advisories/GHSA-p24m-863f-fm6q, https://gith	A-STA-STAR-270223/1304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to consume a large amount of CPU time and RAM. The multipart body parser processes an unlimited number of file parts and an unlimited number of field parts. This is a remote, potentially unauthenticated Denial of Service vulnerability. This vulnerability affects applications with a request handler that accepts a `Body(media_type=RequestEncodingType.MULTI_PART)`. The large amount of CPU time required for processing requests can block all available worker processes and significantly delay or slow down the processing of legitimate user requests. The large amount of RAM accumulated while processing requests can lead to Out-Of-Memory kills. Complete DoS is achievable by sending many concurrent multipart requests in a loop. Version 1.51.2 contains a patch for this issue. **CVE ID : CVE-2023-25578**	ub.com/starlite-api/starlite/commit/9674fe803628f986c03fe60769048cbc55b5bf83	
Vendor: switcherapi					
Product: switcher_client					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.1.4					
N/A	03-Feb-2023	7.5	Switcher Client is a JavaScript SDK to work with Switcher API which is cloud-based Feature Flag. Unsanitized input flows into Strategy match operation (EXIST), where it is used to build a regular expression. This may result in a Regular expression Denial of Service attack (reDOS). This issue has been patched in version 3.1.4. As a workaround, avoid using Strategy settings that use REGEX in conjunction with EXIST and NOT_EXIST operations. **CVE ID : CVE-2023-23925**	https://github.com/switcherapi/switcher-client-master/security/advisories/GHSA-wqxw-8h5g-hq56	A-SWI-SWIT-270223/1305
Vendor: synopsys					
Product: coverity					
Affected Version(s): * Up to (excluding) 2022.12.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	6.1	Versions of Coverity Connect prior to 2022.12.0 are vulnerable to an unauthenticated Cross-Site Scripting vulnerability. Any web service hosted on the same sub domain can set a cookie for the whole subdomain which can be used to bypass other mitigations in place for malicious purposes.	https://community.synopsys.com/s/article/SIG-Product-Security-Advisory-CVE-2023-23849-affecting-Coverity	A-SYN-COVE-270223/1306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C **CVE ID : CVE-2023-23849**		
Vendor: templatesnext					
Product: templatesnext_toolkit					
Affected Version(s): * Up to (excluding) 3.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	The TemplatesNext ToolKit WordPress plugin before 3.2.9 does not validate some of its shortcode attributes before using them to generate an HTML tag, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0333**	N/A	A-TEM-TEMP-270223/1307
Vendor: Tenable					
Product: nessus					
Affected Version(s): -					
N/A	01-Feb-2023	8.8	As part of our Security Development Lifecycle, a potential privilege escalation issue was identified internally. This could allow a malicious actor with sufficient permissions to modify environment variables and abuse an impacted plugin in order to escalate privileges. We have resolved the issue and also made several defense-in-depth fixes	https://www.tenable.com/security/tns-2023-04	A-TEN-NESS-270223/1308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alongside. While the probability of successful exploitation is low, Tenable is committed to securing our customers' environments and our products. The updates have been distributed via the Tenable plugin feed in feed serial numbers equal to or greater than #202212212055. **CVE ID : CVE-2023-0524**		
Product: tenable.io					
Affected Version(s): -					
N/A	01-Feb-2023	8.8	As part of our Security Development Lifecycle, a potential privilege escalation issue was identified internally. This could allow a malicious actor with sufficient permissions to modify environment variables and abuse an impacted plugin in order to escalate privileges. We have resolved the issue and also made several defense-in-depth fixes alongside. While the probability of successful exploitation is low, Tenable is committed to securing our customers' environments and our products. The updates have been distributed	https://www.tenable.com/security/tns-2023-04	A-TEN-TENA-270223/1309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via the Tenable plugin feed in feed serial numbers equal to or greater than #202212212055. **CVE ID : CVE-2023-0524**		
Product: tenable.sc					
Affected Version(s): -					
N/A	01-Feb-2023	8.8	As part of our Security Development Lifecycle, a potential privilege escalation issue was identified internally. This could allow a malicious actor with sufficient permissions to modify environment variables and abuse an impacted plugin in order to escalate privileges. We have resolved the issue and also made several defense-in-depth fixes alongside. While the probability of successful exploitation is low, Tenable is committed to securing our customers' environments and our products. The updates have been distributed via the Tenable plugin feed in feed serial numbers equal to or greater than #202212212055. **CVE ID : CVE-2023-0524**	https://www.tenable.com/security/tns-2023-04	A-TEN-TENA-270223/1310
Vendor: themeum					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: tutor_lms					
Affected Version(s): * Up to (excluding) 2.0.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	6.1	The Tutor LMS WordPress plugin before 2.0.10 does not sanitise and escape the reset_key and user_id parameters before outputting then back in attributes, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-0236**	N/A	A-THE-TUTO-270223/1311
Vendor: themify					
Product: portfolio_post					
Affected Version(s): * Up to (excluding) 1.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	Themify Portfolio Post WordPress plugin before 1.2.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0362**	N/A	A-THE-PORT-270223/1312
Vendor: timescale					
Product: timescaledb					
Affected Version(s): From (including) 2.8.0 Up to (including) 2.9.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	14-Feb-2023	8.8	TimescaleDB, an open-source time-series SQL database, has a privilege escalation vulnerability in versions 2.8.0 through 2.9.2. During installation, TimescaleDB creates a telemetry job that is runs as the installation user. The queries run as part of the telemetry data collection were not run with a locked down `search_path`, allowing malicious users to create functions that would be executed by the telemetry job, leading to privilege escalation. In order to be able to take advantage of this vulnerability, a user would need to be able to create objects in a database and then get a superuser to install TimescaleDB into their database. When TimescaleDB is installed as trusted extension, non-superusers can install the extension without help from a superuser. Version 2.9.3 fixes this issue. As a mitigation, the `search_path` of the user running the telemetry job can be locked down to not include schemas	https://github.com/timescale/timescaledb/pull/5259	A-TIM-TIME-270223/1313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			writable by other users. The vulnerability is not exploitable on instances in Timescale Cloud and Managed Service for TimescaleDB due to additional security provisions in place on those platforms. **CVE ID : CVE-2023-25149**		
Vendor: tina					
Product: tinacms					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.0.9					
Exposure of Sensitive Information to an Unauthorized Actor	08-Feb-2023	7.5	Tinacms is a Git-backed headless content management system with support for visual editing. Sites being built with @tinacms/cli >= 1.0.0 && < 1.0.9 which store sensitive values in the process.env variable are impacted. These values will be added in plaintext to the index.js file. If you're on a version prior to 1.0.0 this vulnerability does not affect you. If you are affected and your Tina-enabled website has sensitive credentials stored as environment variables (eg. Algolia API keys) you should rotate those keys immediately. This issue has been patched in @tinacms/cli@1.0.9. Users are advised to	https://github.com/tinacms/tinacms/pull/3584, https://github.com/tinacms/tinacms/security/advisories/GHSA-pc2q-jcxq-rjrr	A-TIN-TINA-270223/1314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-25164**		
Vendor: Tipsandtricks-hq					
Product: easy_accept_payments_for_paypal					
Affected Version(s): * Up to (excluding) 4.9.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	The Easy Accept Payments for PayPal WordPress plugin before 4.9.10 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0275**	N/A	A-TIP-EASY-270223/1315
Vendor: trellix					
Product: data_loss_prevention					
Affected Version(s): From (including) 11.9.0 Up to (excluding) 11.10.0					
Uncontrolled Search Path Element	02-Feb-2023	8.2	The protection bypass vulnerability in DLP for Windows 11.9.x is addressed in version 11.10.0. This allowed a local user to bypass DLP controls when uploading sensitive data from a mapped drive into a web email client. Loading from a local driver was correctly prevented.	https://kcm.trellix.com/corporate/index?page=content&id=SB10394&locale=en_US	A-TRE-DATA-270223/1316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Versions prior to 11.9 correctly detected and blocked the attempted upload of sensitive data. **CVE ID : CVE-2023-0400**		
Vendor: Trendmicro					
Product: apex_one					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	01-Feb-2023	9.1	A file upload vulnerability in exists in Trend Micro Apex One server build 11110. Using a malformed Content-Length header in an HTTP PUT message sent to URL /officescan/console/html/cgi/fcgiOfcDDA.exe, an unauthenticated remote attacker can upload arbitrary files to the SampleSubmission directory (i.e., \PCCSRV\TEMP\SampleSubmission) on the server. The attacker can upload a large number of large files to fill up the file system on which the Apex One server is installed. **CVE ID : CVE-2023-0587**	N/A	A-TRE-APEX-270223/1317
Vendor: twinpictures					
Product: annual_archive					
Affected Version(s): * Up to (excluding) 1.6.0					
Improper Neutralization of Input	06-Feb-2023	5.4	The Annual Archive WordPress plugin before 1.6.0 does not validate and escape	N/A	A-TWI-ANNU-270223/1318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0178**		
Product: jquery_t\(-\)_countdown_widget					
Affected Version(s): * Up to (excluding) 2.3.34					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The jQuery T(-) Countdown Widget WordPress plugin before 2.3.24 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0171**	N/A	A-TWI-JQUE-270223/1319
Vendor: Typo3					
Product: typo3					
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.4.36					
Improper Neutralization of Input During Web Page Generation	07-Feb-2023	6.1	TYPO3 is a free and open source Content Management Framework released under the GNU General Public License. In affected versions the	https://typo3.org/security/advisory/typo3-psa-2023-001, https://github.com/TYP	A-TYP-TYPO-270223/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			TYPO3 core component `GeneralUtility::getIndpEnv()` uses the unfiltered server environment variable `PATH_INFO`, which allows attackers to inject malicious content. In combination with the TypoScript setting `config.absRefPrefix=auto`, attackers can inject malicious HTML code to pages that have not been rendered and cached, yet. As a result, injected values would be cached and delivered to other website visitors (persisted cross-site scripting). Individual code which relies on the resolved value of `GeneralUtility::getIndpEnv('SCRIPT_NAME')` and corresponding usages (as shown below) are vulnerable as well. Additional investigations confirmed that at least Apache web server deployments using CGI (FPM, FCGI/FastCGI, and similar) are affected. However, there still might be the risk that other scenarios like nginx, IIS, or Apache/mod_php are vulnerable. The usage of server	O3/typo3/commit/0005a6fd86ab97eff8bf2e3a5828bf0e7cb6263a, https://github.com/TYPO3/typo3/security/advisories/GHSA-r4f8-f93x-5qh3	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			environment variable `PATH_INFO` has been removed from corresponding processings in `GeneralUtility::getIndpEnv()`. Besides that, the public property `TypoScriptFrontendController::$absRefPrefix` is encoded for both being used as a URI component and for being used as a prefix in an HTML context. This mitigates the cross-site scripting vulnerability. Users are advised to update to TYPO3 versions 8.7.51 ELTS, 9.5.40 ELTS, 10.4.35 LTS, 11.5.23 LTS and 12.2.0 which fix this problem. For users who are unable to patch in a timely manner the TypoScript setting `config.absRefPrefix` should at least be set to a static path value, instead of using auto - e.g. `config.absRefPrefix=/`. This workaround **does not fix all aspects of the vulnerability**, and is just considered to be an intermediate mitigation to the most prominent manifestation. **CVE ID : CVE-2023-24814**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 11.0.0 Up to (excluding) 11.5.23					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Feb-2023	6.1	TYPO3 is a free and open source Content Management Framework released under the GNU General Public License. In affected versions the TYPO3 core component `GeneralUtility::getIndpEnv()` uses the unfiltered server environment variable `PATH_INFO`, which allows attackers to inject malicious content. In combination with the TypoScript setting `config.absRefPrefix=auto`, attackers can inject malicious HTML code to pages that have not been rendered and cached, yet. As a result, injected values would be cached and delivered to other website visitors (persisted cross-site scripting). Individual code which relies on the resolved value of `GeneralUtility::getIndpEnv('SCRIPT_NAME')` and corresponding usages (as shown below) are vulnerable as well. Additional investigations confirmed that at least Apache web server deployments using CGI (FPM, FCGI/FastCGI,	https://typo3.org/security/advisory/typo3-psa-2023-001, https://github.com/TYPO3/typo3/commit/0005a6fd86ab97eff8bf2e3a5828bf0e7cb6263a, https://github.com/TYPO3/typo3/security/advisories/GHSA-r4f8-f93x-5qh3	A-TYP-TYPO-270223/1321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and similar) are affected. However, there still might be the risk that other scenarios like nginx, IIS, or Apache/mod_php are vulnerable. The usage of server environment variable `PATH_INFO` has been removed from corresponding processings in `GeneralUtility::getIndpEnv()`. Besides that, the public property `TypoScriptFrontendController::$absRefPrefix` is encoded for both being used as a URI component and for being used as a prefix in an HTML context. This mitigates the cross-site scripting vulnerability. Users are advised to update to TYPO3 versions 8.7.51 ELTS, 9.5.40 ELTS, 10.4.35 LTS, 11.5.23 LTS and 12.2.0 which fix this problem. For users who are unable to patch in a timely manner the TypoScript setting `config.absRefPrefix` should at least be set to a static path value, instead of using auto - e.g. `config.absRefPrefix=/`. This workaround **does not fix all aspects of the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability**, and is just considered to be an intermediate mitigation to the most prominent manifestation. **CVE ID : CVE-2023-24814**		
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Feb-2023	6.1	TYPO3 is a free and open source Content Management Framework released under the GNU General Public License. In affected versions the TYPO3 core component `GeneralUtility::getIndpEnv()` uses the unfiltered server environment variable `PATH_INFO`, which allows attackers to inject malicious content. In combination with the TypoScript setting `config.absRefPrefix=auto`, attackers can inject malicious HTML code to pages that have not been rendered and cached, yet. As a result, injected values would be cached and delivered to other website visitors (persisted cross-site scripting). Individual code which relies on the resolved value of `GeneralUtility::getIndpEnv('SCRIPT_NAME')` and corresponding	https://typo3.org/security/advisory/typo3-psa-2023-001, https://github.com/TYPO3/typo3/commit/0005a6fd86ab97eff8bf2e3a5828bf0e7cb6263a, https://github.com/TYPO3/typo3/security/advisories/GHSA-r4f8-f93x-5qh3	A-TYP-TYPO-270223/1322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			usages (as shown below) are vulnerable as well. Additional investigations confirmed that at least Apache web server deployments using CGI (FPM, FCGI/FastCGI, and similar) are affected. However, there still might be the risk that other scenarios like nginx, IIS, or Apache/mod_php are vulnerable. The usage of server environment variable `PATH_INFO` has been removed from corresponding processings in `GeneralUtility::getIndpEnv()`. Besides that, the public property `TypoScriptFrontendController::$absRefPrefix` is encoded for both being used as a URI component and for being used as a prefix in an HTML context. This mitigates the cross-site scripting vulnerability. Users are advised to update to TYPO3 versions 8.7.51 ELTS, 9.5.40 ELTS, 10.4.35 LTS, 11.5.23 LTS and 12.2.0 which fix this problem. For users who are unable to patch in a timely manner the TypoScript setting `config.absRefPrefix`		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should at least be set to a static path value, instead of using auto - e.g. `config.absRefPrefix=/`. This workaround **does not fix all aspects of the vulnerability**, and is just considered to be an intermediate mitigation to the most prominent manifestation. **CVE ID : CVE-2023-24814**		
Affected Version(s): From (including) 8.7.0 Up to (excluding) 9.7.51					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Feb-2023	6.1	TYPO3 is a free and open source Content Management Framework released under the GNU General Public License. In affected versions the TYPO3 core component `GeneralUtility::getIndpEnv()` uses the unfiltered server environment variable `PATH_INFO`, which allows attackers to inject malicious content. In combination with the TypoScript setting `config.absRefPrefix=auto`, attackers can inject malicious HTML code to pages that have not been rendered and cached, yet. As a result, injected values would be cached and delivered to other website	https://typo3.org/security/advisory/typo3-psa-2023-001, https://github.com/TYPO3/typo3/commit/0005a6fd86ab97eff8bf2e3a5828bf0e7cb6263a, https://github.com/TYPO3/typo3/security/advisories/GHSA-r4f8-f93x-5qh3	A-TYP-TYPO-270223/1323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			visitors (persisted cross-site scripting). Individual code which relies on the resolved value of `GeneralUtility::getIndpEnv('SCRIPT_NAME')` and corresponding usages (as shown below) are vulnerable as well. Additional investigations confirmed that at least Apache web server deployments using CGI (FPM, FCGI/FastCGI, and similar) are affected. However, there still might be the risk that other scenarios like nginx, IIS, or Apache/mod_php are vulnerable. The usage of server environment variable `PATH_INFO` has been removed from corresponding processings in `GeneralUtility::getIndpEnv()`. Besides that, the public property `TypoScriptFrontendController::$absRefPrefix` is encoded for both being used as a URI component and for being used as a prefix in an HTML context. This mitigates the cross-site scripting vulnerability. Users are advised to update to TYPO3 versions 8.7.51 ELTS,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.5.40 ELTS, 10.4.35 LTS, 11.5.23 LTS and 12.2.0 which fix this problem. For users who are unable to patch in a timely manner the TypoScript setting `config.absRefPrefix` should at least be set to a static path value, instead of using auto - e.g. `config.absRefPrefix=/`. This workaround **does not fix all aspects of the vulnerability**, and is just considered to be an intermediate mitigation to the most prominent manifestation. **CVE ID : CVE-2023-24814**		
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.5.40					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Feb-2023	6.1	TYPO3 is a free and open source Content Management Framework released under the GNU General Public License. In affected versions the TYPO3 core component `GeneralUtility::getIndpEnv()` uses the unfiltered server environment variable `PATH_INFO`, which allows attackers to inject malicious content. In combination with the TypoScript setting `config.absRefPrefix=au	https://typo3.org/security/advisory/typo3-psa-2023-001, https://github.com/TYPO3/typo3/commit/0005a6fd86ab97eff8bf2e3a5828bf0e7cb6263a, https://github.com/TYPO3/typo3/security/advisories/GHSA-	A-TYP-TYPO-270223/1324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to`, attackers can inject malicious HTML code to pages that have not been rendered and cached, yet. As a result, injected values would be cached and delivered to other website visitors (persisted cross-site scripting). Individual code which relies on the resolved value of `GeneralUtility::getIndpEnv('SCRIPT_NAME')` and corresponding usages (as shown below) are vulnerable as well. Additional investigations confirmed that at least Apache web server deployments using CGI (FPM, FCGI/FastCGI, and similar) are affected. However, there still might be the risk that other scenarios like nginx, IIS, or Apache/mod_php are vulnerable. The usage of server environment variable `PATH_INFO` has been removed from corresponding processings in `GeneralUtility::getIndpEnv()`. Besides that, the public property `TypoScriptFrontendController::$absRefPrefix` is encoded for both being used as a URI	r4f8-f93x-5qh3	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component and for being used as a prefix in an HTML context. This mitigates the cross-site scripting vulnerability. Users are advised to update to TYPO3 versions 8.7.51 ELTS, 9.5.40 ELTS, 10.4.35 LTS, 11.5.23 LTS and 12.2.0 which fix this problem. For users who are unable to patch in a timely manner the TypoScript setting `config.absRefPrefix` should at least be set to a static path value, instead of using auto - e.g. `config.absRefPrefix=/`. This workaround **does not fix all aspects of the vulnerability**, and is just considered to be an intermediate mitigation to the most prominent manifestation. **CVE ID : CVE-2023-24814**		
Vendor: ureport_project					
Product: ureport					
Affected Version(s): 2.2.9					
Improper Limitation of a Pathname to a Restricted Directory	13-Feb-2023	9.1	ureport v2.2.9 was discovered to contain a directory traversal vulnerability via the deletion function which allows for arbitrary files to be deleted.	N/A	A-URE-UREP-270223/1325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			**CVE ID : CVE-2023-24188**		
Improper Restriction of XML External Entity Reference	14-Feb-2023	7.8	An XML External Entity (XXE) vulnerability in ureport v2.2.9 allows attackers to execute arbitrary code via uploading a crafted XML file to /ureport/designer/saveReportFile. **CVE ID : CVE-2023-24187**	N/A	A-URE-UREP-270223/1326
Vendor: utubevideo_gallery_project					
Product: utubevideo_gallery					
Affected Version(s): * Up to (excluding) 2.0.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	The uTubeVideo Gallery WordPress plugin before 2.0.8 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0151**	N/A	A-UTU-UTUB-270223/1327
Vendor: Vbulletin					
Product: vbulletin					
Affected Version(s): 5.6.7					
Deserialization of Untrusted Data	03-Feb-2023	9.8	vBulletin before 5.6.9 PL1 allows an unauthenticated remote attacker to execute arbitrary code via a	https://forum.vbulletin.com/forum/vbulletin-announceme	A-VBU-VBUL-270223/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request that triggers deserialization. This occurs because verify_serialized checks that a value is serialized by calling unserialize and then checking for errors. The fixed versions are 5.6.7 PL1, 5.6.8 PL1, and 5.6.9 PL1. **CVE ID : CVE-2023-25135**	nts/vbulletin-announcements_aa/4473890-vbulletin-5-6-9-security-patch	
Affected Version(s): 5.6.8					
Deserialization of Untrusted Data	03-Feb-2023	9.8	vBulletin before 5.6.9 PL1 allows an unauthenticated remote attacker to execute arbitrary code via a crafted HTTP request that triggers deserialization. This occurs because verify_serialized checks that a value is serialized by calling unserialize and then checking for errors. The fixed versions are 5.6.7 PL1, 5.6.8 PL1, and 5.6.9 PL1. **CVE ID : CVE-2023-25135**	https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4473890-vbulletin-5-6-9-security-patch	A-VBU-VBUL-270223/1329
Affected Version(s): 5.6.9					
Deserialization of Untrusted Data	03-Feb-2023	9.8	vBulletin before 5.6.9 PL1 allows an unauthenticated remote attacker to execute arbitrary code via a crafted HTTP request that triggers	https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-	A-VBU-VBUL-270223/1330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deserialization. This occurs because verify_serialized checks that a value is serialized by calling unserialize and then checking for errors. The fixed versions are 5.6.7 PL1, 5.6.8 PL1, and 5.6.9 PL1. **CVE ID : CVE-2023-25135**	announcements_aa/4473890-vbulletin-5-6-9-security-patch	
Vendor: vilyon					
Product: gallery_factory_lite					
Affected Version(s): * Up to (including) 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The Gallery Factory Lite WordPress plugin through 2.0.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0148**	N/A	A-VIL-GALL-270223/1331
Vendor: vimeo_video_autoplay_automute_project					
Product: vimeo_video_autoplay_automute					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input During Web Page Generation	06-Feb-2023	5.4	The Vimeo Video Autoplay Automute WordPress plugin through 1.0 does not validate and escape some of its shortcode attributes before	N/A	A-VIM-VIME-270223/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0153**		
Vendor: Vmware					
Product: vrealize_operations					
Affected Version(s): From (including) 8.6.0 Up to (including) 8.6.4					
Cross-Site Request Forgery (CSRF)	01-Feb-2023	8.8	VMware vRealize Operations (vROps) contains a CSRF bypass vulnerability. A malicious user could execute actions on the vROps platform on behalf of the authenticated victim user. **CVE ID : CVE-2023-20856**	https://www.vmware.com/security/advisories/VMSA-2023-0002.html	A-VMW-VREA-270223/1333
Product: workstation					
Affected Version(s): 17.0					
Improper Privilege Management	03-Feb-2023	8.4	VMware Workstation contains an arbitrary file deletion vulnerability. A malicious actor with local user privileges on the victim's machine may exploit this vulnerability to delete arbitrary files from the file system of the machine on which Workstation is installed.	https://www.vmware.com/security/advisories/VMSA-2023-0003.html	A-VMW-WORK-270223/1334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20854		
Vendor: wallabag					
Product: wallabag					
Affected Version(s): * Up to (excluding) 2.5.3					
Improper Authorization	01-Feb-2023	4.3	Improper Authorization in GitHub repository wallabag/wallabag prior to 2.5.3. **CVE ID : CVE-2023-0609**	https://github.com/wallabag/wallabag/commit/0f7460dbab9e29f4f7d2944aca20210f828b6abb, https://huntr.dev/bounties/3adef66f-fc86-4e6d-a540-2ffa59342ff0	A-WAL-WALL-270223/1335
Improper Authorization	01-Feb-2023	4.3	Improper Authorization in GitHub repository wallabag/wallabag prior to 2.5.3. **CVE ID : CVE-2023-0610**	https://github.com/wallabag/wallabag/commit/5ac6b6bff9e2e3a87fd88c2904ff3c6aac40722e, https://huntr.dev/bounties/8fdd9b31-d89b-4bbe-9557-20b960faf926	A-WAL-WALL-270223/1336
Affected Version(s): * Up to (excluding) 2.5.4					
Cross-Site Request Forgery (CSRF)	07-Feb-2023	6.5	Cross-Site Request Forgery (CSRF) in GitHub repository wallabag/wallabag prior to 2.5.4.	https://github.com/wallabag/wallabag/commit/268372dbbdd7ef87b84617fdebf95d0	A-WAL-WALL-270223/1337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0735	a86caf7dc, https://huntr.dev/bounties/8bc78cb1-b10b-4152-842e-ceb999fc5508	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Feb-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository wallabag/wallabag prior to 2.5.4. **CVE ID : CVE-2023-0736**	https://huntr.dev/bounties/7e6f9614-6a96-4295-83f0-06a240be844e, https://github.com/wallabag/wallabag/commit/4e023bddc3622ba5e901cc14a261fcb98d955cd7	A-WAL-WALL-270223/1338
Vendor: wallix					
Product: bastion_access_manager					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.16					
N/A	09-Feb-2023	7.5	WALLIX Access Manager 3.x through 4.0.x allows a remote attacker to access sensitive information. **CVE ID : CVE-2023-23592**	https://www.wallix.com/support/alerts/	A-WAL-BAST-270223/1339
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.3					
N/A	09-Feb-2023	7.5	WALLIX Access Manager 3.x through 4.0.x allows a remote attacker to access sensitive information. **CVE ID : CVE-2023-23592**	https://www.wallix.com/support/alerts/	A-WAL-BAST-270223/1340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wcvendors					
Product: wc_vendors_marketplace					
Affected Version(s): * Up to (excluding) 2.4.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The WC Vendors Marketplace WordPress plugin before 2.4.5 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0072**	N/A	A-WCV-WC_V-270223/1341
Vendor: webberzone					
Product: contextual_related_posts					
Affected Version(s): * Up to (excluding) 3.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The Contextual Related Posts WordPress plugin before 3.3.1 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0252**	N/A	A-WEB-CONT-270223/1342
Vendor: wickedplugins					
Product: wicked_folders					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.18.16					
Missing Authorization	08-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_unassign_folders function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as changing the folder structure maintained by the plugin. **CVE ID : CVE-2023-0684**	N/A	A-WIC-WICK-270223/1343
Cross-Site Request Forgery (CSRF)	08-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.18.16. This is due to missing or incorrect nonce validation on the ajax_unassign_folders function. This makes it possible for unauthenticated attackers to invoke this function via forged request granted they can trick a site administrator into performing an action	N/A	A-WIC-WICK-270223/1344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such as clicking on a link leading them to perform actions intended for administrators such as changing the folder structure maintained by the plugin.. **CVE ID : CVE-2023-0685**		
Missing Authorization	08-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_save_state function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as modifying the view state of the folder structure maintained by the plugin. **CVE ID : CVE-2023-0711**	N/A	A-WIC-WICK-270223/1345
Missing Authorization	07-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_move_object function in versions up to, and including, 2.18.16. This makes it	N/A	A-WIC-WICK-270223/1346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as modifying the folder structure maintained by the plugin. **CVE ID : CVE-2023-0712**		
Missing Authorization	07-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_add_folder function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as modifying the folder structure maintained by the plugin. **CVE ID : CVE-2023-0713**	N/A	A-WIC-WICK-270223/1347
Missing Authorization	08-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_clone_folder	N/A	A-WIC-WICK-270223/1348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as modifying the folder structure maintained by the plugin. **CVE ID : CVE-2023-0715**		
Missing Authorization	08-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_edit_folder function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as modifying the folder structure maintained by the plugin. **CVE ID : CVE-2023-0716**	N/A	A-WIC-WICK-270223/1349
Missing Authorization	08-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass	N/A	A-WIC-WICK-270223/1350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a missing capability check on the ajax_delete_folder function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as modifying the folder structure maintained by the plugin. **CVE ID : CVE-2023-0717**		
Missing Authorization	08-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_save_folder function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as modifying the folder structure maintained by the plugin. **CVE ID : CVE-2023-0718**	N/A	A-WIC-WICK-270223/1351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	07-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_save_sort_order function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as modifying the folder structure maintained by the plugin. **CVE ID : CVE-2023-0719**	N/A	A-WIC-WICK-270223/1352
Missing Authorization	08-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_save_folder_order function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as modifying the folder	N/A	A-WIC-WICK-270223/1353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			structure maintained by the plugin. **CVE ID : CVE-2023-0720**		
Cross-Site Request Forgery (CSRF)	08-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.18.16. This is due to missing or incorrect nonce validation on the ajax_save_state function. This makes it possible for unauthenticated attackers to invoke this function via forged request granted they can trick a site administrator into performing an action such as clicking on a link leading them to perform actions intended for administrators such as changing the folder structure maintained by the plugin. **CVE ID : CVE-2023-0722**	N/A	A-WIC-WICK-270223/1354
Cross-Site Request Forgery (CSRF)	07-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.18.16. This is due to missing or incorrect nonce validation on the ajax_move_object	N/A	A-WIC-WICK-270223/1355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function. This makes it possible for unauthenticated attackers to invoke this function via forged request granted they can trick a site administrator into performing an action such as clicking on a link leading them to perform actions intended for administrators such as changing the folder structure maintained by the plugin. **CVE ID : CVE-2023-0723**		
Cross-Site Request Forgery (CSRF)	08-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.18.16. This is due to missing or incorrect nonce validation on the ajax_add_folder function. This makes it possible for unauthenticated attackers to invoke this function via forged request granted they can trick a site administrator into performing an action such as clicking on a link leading them to perform actions intended for administrators such as	N/A	A-WIC-WICK-270223/1356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			changing the folder structure maintained by the plugin. **CVE ID : CVE-2023-0724**		
Cross-Site Request Forgery (CSRF)	08-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.18.16. This is due to missing or incorrect nonce validation on the ajax_clone_folder function. This makes it possible for unauthenticated attackers to invoke this function via forged request granted they can trick a site administrator into performing an action such as clicking on a link leading them to perform actions intended for administrators such as changing the folder structure maintained by the plugin. **CVE ID : CVE-2023-0725**	N/A	A-WIC-WICK-270223/1357
Cross-Site Request Forgery (CSRF)	08-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.18.16. This is due to missing or incorrect nonce validation on the	N/A	A-WIC-WICK-270223/1358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ajax_edit_folder function. This makes it possible for unauthenticated attackers to invoke this function via forged request granted they can trick a site administrator into performing an action such as clicking on a link leading them to perform actions intended for administrators such as changing the folder structure maintained by the plugin. **CVE ID : CVE-2023-0726**		
Cross-Site Request Forgery (CSRF)	07-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.18.16. This is due to missing or incorrect nonce validation on the ajax_delete_folder function. This makes it possible for unauthenticated attackers to invoke this function via forged request granted they can trick a site administrator into performing an action such as clicking on a link leading them to perform actions intended for	N/A	A-WIC-WICK-270223/1359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrators such as changing the folder structure maintained by the plugin. **CVE ID : CVE-2023-0727**		
Cross-Site Request Forgery (CSRF)	07-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.18.16. This is due to missing or incorrect nonce validation on the ajax_save_folder function. This makes it possible for unauthenticated attackers to invoke this function via forged request granted they can trick a site administrator into performing an action such as clicking on a link leading them to perform actions intended for administrators such as changing the folder structure maintained by the plugin. **CVE ID : CVE-2023-0728**	N/A	A-WIC-WICK-270223/1360
Cross-Site Request Forgery (CSRF)	07-Feb-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.18.16. This is due to missing or incorrect nonce	N/A	A-WIC-WICK-270223/1361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation on the ajax_save_folder_order function. This makes it possible for unauthenticated attackers to invoke this function via forged request granted they can trick a site administrator into performing an action such as clicking on a link leading them to perform actions intended for administrators such as changing the folder structure maintained by the plugin. **CVE ID : CVE-2023-0730**		
Vendor: wordprezi_project					
Product: wordprezi					
Affected Version(s): * Up to (including) 0.8.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The WordPrezi WordPress plugin through 0.8.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0149**	N/A	A-WOR-WORD-270223/1362
Vendor: wpdevart					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: social_like_box_and_page					
Affected Version(s): * Up to (excluding) 0.8.41					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	The Social Like Box and Page by WpDevArt WordPress plugin before 0.8.41 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0177**	N/A	A-WPD-SOCI-270223/1363
Vendor: wpfactory					
Product: ean_for_woocommerce					
Affected Version(s): * Up to (excluding) 4.4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-2023	5.4	The EAN for WooCommerce WordPress plugin before 4.4.3 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0062**	N/A	A-WPF-EAN_-270223/1364
Vendor: wprealize					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: extensive_vc_addons_for_wpbakery_page_builder					
Affected Version(s): * Up to (excluding) 1.9.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Feb-2023	7.5	The Extensive VC Addons for WPBakery page builder WordPress plugin before 1.9.1 does not validate a parameter passed to the php extract function when loading templates, allowing an unauthenticated attacker to override the template path to read arbitrary files from the hosts file system. **CVE ID : CVE-2023-0159**	N/A	A-WPR-EXTE-270223/1365
Vendor: xuxueli					
Product: xxl-job					
Affected Version(s): 2.3.1					
Cross-Site Request Forgery (CSRF)	04-Feb-2023	6.5	A vulnerability, which was classified as problematic, has been found in XXL-JOB 2.3.1. Affected by this issue is some unknown functionality of the file /user/updatePwd of the component New Password Handler. The manipulation leads to cross-site request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-220196.	N/A	A-XUX-XXL--270223/1366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0674		
Vendor: yamaps_project					
Product: yamaps					
Affected Version(s): * Up to (excluding) 0.6.26					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	5.4	The YaMaps for WordPress Plugin WordPress plugin before 0.6.26 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0270**	N/A	A-YAM-YAMA-270223/1367
Vendor: yetanotherforum					
Product: yaf.net					
Affected Version(s): * Up to (including) 3.1.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Feb-2023	5.4	A vulnerability was found in YAFNET up to 3.1.11 and classified as problematic. This issue affects some unknown processing of the component Signature Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.1.12 is able to	https://github.com/YAFNET/YAFNET/commit/a1442a2bacc3335461b44c250e81f8d99c60735f	A-YET-YAF.-270223/1368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address this issue. The name of the patch is a1442a2bacc3335461b44c250e81f8d99c60735f. It is recommended to upgrade the affected component. The identifier VDB-220037 was assigned to this vulnerability. **CVE ID : CVE-2023-0650**		
Vendor: yugabyte					
Product: yugabytedb					
Affected Version(s): * Up to (excluding) 2.2.0.0					
N/A	09-Feb-2023	9.8	External Control of Critical State Data, Improper Control of Generation of Code ('Code Injection') vulnerability in YugaByte, Inc. Yugabyte DB on Windows, Linux, MacOS, iOS (DevopsBase.Java:execCommand, TableManager.Java:runCommand modules) allows API Manipulation, Privilege Abuse. This vulnerability is associated with program files backup.Py. This issue affects Yugabyte DB: Lesser then 2.2. **CVE ID : CVE-2023-0575**	N/A	A-YUG-YUGA-270223/1369
Product: yugabytedb_managed					
Affected Version(s): From (including) 2.0 Up to (including) 2.13					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Feb-2023	9.8	Server-Side Request Forgery (SSRF), Improperly Controlled Modification of Dynamically-Determined Object Attributes, Improper Restriction of Excessive Authentication Attempts vulnerability in YugaByte, Inc. Yugabyte Managed allows Accessing Functionality Not Properly Constrained by ACLs, Communication Channel Manipulation, Authentication Abuse.This issue affects Yugabyte Managed: from 2.0 through 2.13. **CVE ID : CVE-2023-0574**	N/A	A-YUG-YUGA-270223/1370
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Feb-2023	9.8	Relative Path Traversal vulnerability in YugaByte, Inc. Yugabyte Managed (PlatformReplicationManager.Java modules) allows Path Traversal. This vulnerability is associated with program files PlatformReplicationManager.Java. This issue affects Yugabyte Managed: from 2.0 through 2.13. **CVE ID : CVE-2023-0745**	N/A	A-YUG-YUGA-270223/1371
Vendor: zippy					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: zstore					
Affected Version(s): 6.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Feb-2023	6.1	Zstore v6.6.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /index.php. **CVE ID : CVE-2023-24648**	N/A	A-ZIP-ZSTO-270223/1372
Vendor: Zohocorp					
Product: manageengine_assetexplorer					
Affected Version(s): 6.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Feb-2023	6.1	Cross Site Scripting (XSS) vulnerability in Zoho Asset Explorer 6.9 via the credential name when creating a new Assets Workstation. **CVE ID : CVE-2023-23075**	https://bugbounty.zohocorp.com/bb/#/bug/1010000064630 45?tab=originator	A-ZOH-MANA-270223/1373
Product: manageengine_servicedesk_plus					
Affected Version(s): 13.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Feb-2023	6.1	Cross site scripting (XSS) vulnerability in Zoho ManageEngine ServiceDesk Plus 13 via the comment field when adding a new status comment. **CVE ID : CVE-2023-23077**	https://bugbounty.zohocorp.com/bb/#/bug/1010000063876 93?tab=originator	A-ZOH-MANA-270223/1374
Affected Version(s): 14.0					
Improper Neutralization of Input During	01-Feb-2023	6.1	Cross site scripting (XSS) vulnerability in Zoho ManageEngine ServiceDesk Plus 14 via	https://bugbounty.zohocorp.com/bb/#/bug/1010000064591	A-ZOH-MANA-270223/1375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			PO in the purchase component. **CVE ID : CVE-2023-23073**	71?tab=originator	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Feb-2023	6.1	Cross site scripting (XSS) vulnerability in Zoho ManageEngine ServiceDesk Plus 14 via embedding videos in the language component. **CVE ID : CVE-2023-23074**	https://bugbounty.zohocorp.com/bb/#/bug/1010000064591 95?tab=originator	A-ZOH-MANA-270223/1376
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Feb-2023	6.1	Cross site scripting (XSS) vulnerability in Zoho ManageEngine ServiceDesk Plus 14 via the comment field when changing the credentials in the Assets. **CVE ID : CVE-2023-23078**	https://bugbounty.zohocorp.com/bb/#/bug/1010000064586 75?tab=originator	A-ZOH-MANA-270223/1377
Product: manageengine_supportcenter_plus					
Affected Version(s): 11.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Feb-2023	9.8	OS Command injection vulnerability in Support Center Plus 11 via Executor in Action when creating new schedules. **CVE ID : CVE-2023-23076**	N/A	A-ZOH-MANA-270223/1378
Product: zoho_forms					
Affected Version(s): * Up to (excluding) 3.0.1					
Improper Neutralizat	13-Feb-2023	5.4	The Zoho Forms WordPress plugin	N/A	A-ZOH-ZOHO-270223/1379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			before 3.0.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0169**		
Vendor: Zulip					
Product: zulip_server					
Affected Version(s): 2023-01-09					
Interpretation Conflict	07-Feb-2023	4.6	Zulip is an open-source team collaboration tool. In versions of zulip prior to commit `2f6c5a8` but after commit `04cf68b` users could upload files with arbitrary `Content-Type` which would be served from the Zulip hostname with `Content-Disposition: inline` and no `Content-Security-Policy` header, allowing them to trick other users into executing arbitrary Javascript in the context of the Zulip application. Among other things, this enables session theft. Only deployments which use the S3 storage (not the local-disk storage) are	https://github.com/zulip/zulip/commit/2f6c5a883e106aa82a570d3d1f243993284b70f3, https://github.com/zulip/zulip/security/advisories/GHSA-wm83-3764-5wqh	A-ZUL-ZULI-270223/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected, and only deployments which deployed commit 04cf68b45ebb5c03247a0d6453e35ffc175d55da, which has only been in `main`, not any numbered release. Users affected should upgrade from main again to deploy this fix. Switching from S3 storage to the local-disk storage would nominally mitigate this, but is likely more involved than upgrading to the latest `main` which addresses the issue. **CVE ID : CVE-2023-22735**		
Hardware					
Vendor: arraynetworks					
Product: ag1000					
Affected Version(s): -					
Out-of-bounds Write	03-Feb-2023	4.9	The user interface of Array Networks AG Series and vxAG through 9.4.0.470 could allow a remote attacker to use the gdb tool to overwrite the backend function call stack after accessing the system with administrator privileges. A successful exploit could leverage this vulnerability in the backend binary file that handles the user interface to a cause	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_UI_Stack_Overflow_Vulnerability_ID-	H-ARR-AG10-270223/1381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service attack. This is fixed in AG 9.4.0.481. **CVE ID : CVE-2023-24613**	128285_V1.0.pdf	
Product: ag1000t					
Affected Version(s): -					
Out-of-bounds Write	03-Feb-2023	4.9	The user interface of Array Networks AG Series and vxAG through 9.4.0.470 could allow a remote attacker to use the gdb tool to overwrite the backend function call stack after accessing the system with administrator privileges. A successful exploit could leverage this vulnerability in the backend binary file that handles the user interface to a cause denial of service attack. This is fixed in AG 9.4.0.481. **CVE ID : CVE-2023-24613**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_UI_Stack_Overflow_Vulnerability_ID-128285_V1.0.pdf	H-ARR-AG10-270223/1382
Product: ag1000v5					
Affected Version(s): -					
Out-of-bounds Write	03-Feb-2023	4.9	The user interface of Array Networks AG Series and vxAG through 9.4.0.470 could allow a remote attacker to use the gdb tool to overwrite the backend function call stack after accessing the system with administrator privileges. A successful	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Secur	H-ARR-AG10-270223/1383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could leverage this vulnerability in the backend binary file that handles the user interface to a cause denial of service attack. This is fixed in AG 9.4.0.481. **CVE ID : CVE-2023-24613**	ity_Advisory_for_UI_Stack_Overflow_Vulnerability_ID-128285_V1.0.pdf	
Product: ag1100v5					
Affected Version(s): -					
Out-of-bounds Write	03-Feb-2023	4.9	The user interface of Array Networks AG Series and vxAG through 9.4.0.470 could allow a remote attacker to use the gdb tool to overwrite the backend function call stack after accessing the system with administrator privileges. A successful exploit could leverage this vulnerability in the backend binary file that handles the user interface to a cause denial of service attack. This is fixed in AG 9.4.0.481. **CVE ID : CVE-2023-24613**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_UI_Stack_Overflow_Vulnerability_ID-128285_V1.0.pdf	H-ARR-AG11-270223/1384
Product: ag1150					
Affected Version(s): -					
Out-of-bounds Write	03-Feb-2023	4.9	The user interface of Array Networks AG Series and vxAG through 9.4.0.470 could allow a remote attacker to use the gdb tool to	https://support.arraynetworks.net/prx/001/http/supportportal.arraynet	H-ARR-AG11-270223/1385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overwrite the backend function call stack after accessing the system with administrator privileges. A successful exploit could leverage this vulnerability in the backend binary file that handles the user interface to a cause denial of service attack. This is fixed in AG 9.4.0.481. **CVE ID : CVE-2023-24613**	works.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_UI_Stack_Overflow_Vulnerability_ID-128285_V1.0.pdf	
Product: ag1200					
Affected Version(s): -					
Out-of-bounds Write	03-Feb-2023	4.9	The user interface of Array Networks AG Series and vxAG through 9.4.0.470 could allow a remote attacker to use the gdb tool to overwrite the backend function call stack after accessing the system with administrator privileges. A successful exploit could leverage this vulnerability in the backend binary file that handles the user interface to a cause denial of service attack. This is fixed in AG 9.4.0.481. **CVE ID : CVE-2023-24613**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_UI_Stack_Overflow_Vulnerability_ID-128285_V1.0.pdf	H-ARR-AG12-270223/1386
Product: ag1200v5					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Feb-2023	4.9	The user interface of Array Networks AG Series and vxAG through 9.4.0.470 could allow a remote attacker to use the gdb tool to overwrite the backend function call stack after accessing the system with administrator privileges. A successful exploit could leverage this vulnerability in the backend binary file that handles the user interface to a cause denial of service attack. This is fixed in AG 9.4.0.481. **CVE ID : CVE-2023-24613**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_UI_Stack_Overflow_Vulnerability_ID-128285_V1.0.pdf	H-ARR-AG12-270223/1387
Product: ag1500					
Affected Version(s): -					
Out-of-bounds Write	03-Feb-2023	4.9	The user interface of Array Networks AG Series and vxAG through 9.4.0.470 could allow a remote attacker to use the gdb tool to overwrite the backend function call stack after accessing the system with administrator privileges. A successful exploit could leverage this vulnerability in the backend binary file that handles the user interface to a cause denial of service attack. This is fixed in AG 9.4.0.481.	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_UI_Stack_Overflow_Vulnerability_ID-128285_V1.0.pdf	H-ARR-AG15-270223/1388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24613		
Product: ag1500fips					
Affected Version(s): -					
Out-of-bounds Write	03-Feb-2023	4.9	The user interface of Array Networks AG Series and vxAG through 9.4.0.470 could allow a remote attacker to use the gdb tool to overwrite the backend function call stack after accessing the system with administrator privileges. A successful exploit could leverage this vulnerability in the backend binary file that handles the user interface to a cause denial of service attack. This is fixed in AG 9.4.0.481. **CVE ID : CVE-2023-24613**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_UI_Stack_Overflow_Vulnerability_ID-128285_V1.0.pdf	H-ARR-AG15-270223/1389
Product: ag1500v5					
Affected Version(s): -					
Out-of-bounds Write	03-Feb-2023	4.9	The user interface of Array Networks AG Series and vxAG through 9.4.0.470 could allow a remote attacker to use the gdb tool to overwrite the backend function call stack after accessing the system with administrator privileges. A successful exploit could leverage this vulnerability in the backend binary file that handles the user	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_UI_Stack_Overflow_Vulnerability	H-ARR-AG15-270223/1390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface to a cause denial of service attack. This is fixed in AG 9.4.0.481. **CVE ID : CVE-2023-24613**	_ID-128285_V1.0.pdf	
Product: ag1600					
Affected Version(s): -					
Out-of-bounds Write	03-Feb-2023	4.9	The user interface of Array Networks AG Series and vxAG through 9.4.0.470 could allow a remote attacker to use the gdb tool to overwrite the backend function call stack after accessing the system with administrator privileges. A successful exploit could leverage this vulnerability in the backend binary file that handles the user interface to a cause denial of service attack. This is fixed in AG 9.4.0.481. **CVE ID : CVE-2023-24613**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_UI_Stack_Overflow_Vulnerability_ID-128285_V1.0.pdf	H-ARR-AG16-270223/1391
Product: ag1600v5					
Affected Version(s): -					
Out-of-bounds Write	03-Feb-2023	4.9	The user interface of Array Networks AG Series and vxAG through 9.4.0.470 could allow a remote attacker to use the gdb tool to overwrite the backend function call stack after accessing the system with administrator	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Net	H-ARR-AG16-270223/1392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges. A successful exploit could leverage this vulnerability in the backend binary file that handles the user interface to a cause denial of service attack. This is fixed in AG 9.4.0.481. **CVE ID : CVE-2023-24613**	works_Security_Advisory_for_UI_Stack_Overflow_Vulnerability_ID-128285_V1.0.pdf	
Product: vxag					
Affected Version(s): -					
Out-of-bounds Write	03-Feb-2023	4.9	The user interface of Array Networks AG Series and vxAG through 9.4.0.470 could allow a remote attacker to use the gdb tool to overwrite the backend function call stack after accessing the system with administrator privileges. A successful exploit could leverage this vulnerability in the backend binary file that handles the user interface to a cause denial of service attack. This is fixed in AG 9.4.0.481. **CVE ID : CVE-2023-24613**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_UI_Stack_Overflow_Vulnerability_ID-128285_V1.0.pdf	H-ARR-VXAG-270223/1393
Vendor: baicells					
Product: neutrino_430					
Affected Version(s): -					
Improper Neutralization of Special	11-Feb-2023	10	Baicells Nova 436Q, Nova 430E, Nova 430I, and Neutrino 430 LTE TDD eNodeB devices	https://baicells.com/Service/Firmware	H-BAI-NEUT-270223/1394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			with firmware through QRTB 2.12.7 are vulnerable to remote shell code exploitation via HTTP command injections. Commands are executed using pre-login execution and executed with root permissions. The following methods below have been tested and validated by a 3rd party analyst and has been confirmed exploitable special thanks to Rustam Amin for providing the steps to reproduce. **CVE ID : CVE-2023-0776**		
Product: nova430e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Feb-2023	10	Baicells Nova 436Q, Nova 430E, Nova 430I, and Neutrino 430 LTE TDD eNodeB devices with firmware through QRTB 2.12.7 are vulnerable to remote shell code exploitation via HTTP command injections. Commands are executed using pre-login execution and executed with root permissions. The following methods below have been tested and validated by a 3rd party analyst and has been confirmed exploitable special	https://baicells.com/Service/Firmware	H-BAI-NOVA-270223/1395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			thanks to Rustam Amin for providing the steps to reproduce. **CVE ID : CVE-2023-0776**		
Product: nova430l					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Feb-2023	10	Baicells Nova 436Q, Nova 430E, Nova 430I, and Neutrino 430 LTE TDD eNodeB devices with firmware through QRTB 2.12.7 are vulnerable to remote shell code exploitation via HTTP command injections. Commands are executed using pre-login execution and executed with root permissions. The following methods below have been tested and validated by a 3rd party analyst and has been confirmed exploitable special thanks to Rustam Amin for providing the steps to reproduce. **CVE ID : CVE-2023-0776**	https://baicells.com/Service/Firmware	H-BAI-NOVA-270223/1396
Product: nova436q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command	11-Feb-2023	10	Baicells Nova 436Q, Nova 430E, Nova 430I, and Neutrino 430 LTE TDD eNodeB devices with firmware through QRTB 2.12.7 are vulnerable to remote	https://baicells.com/Service/Firmware	H-BAI-NOVA-270223/1397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			shell code exploitation via HTTP command injections. Commands are executed using pre-login execution and executed with root permissions. The following methods below have been tested and validated by a 3rd party analyst and has been confirmed exploitable special thanks to Rustam Amin for providing the steps to reproduce. **CVE ID : CVE-2023-0776**		
Vendor: bdcom					
Product: 1704-wgl					
Affected Version(s): -					
N/A	03-Feb-2023	7.5	A vulnerability was found in BDCOM 1704-WGL 2.0.6314. It has been classified as critical. This affects an unknown part of the file /param.file.tgz of the component Backup File Handler. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The identifier VDB-220101 was assigned to this vulnerability. **CVE ID : CVE-2023-0659**	N/A	H-BDC-1704-270223/1398
Vendor: bosswerk					
Product: inverter					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of Hard-coded Credentials	13-Feb-2023	6.8	A vulnerability was found in Deye/Revolt/Bosswerk Inverter MW3_15U_5406_1.47/ MW3_15U_5406_1.471. It has been rated as problematic. This issue affects some unknown processing of the component Access Point Setting Handler. The manipulation with the input 12345678 leads to use of hard-coded password. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. Upgrading to version MW3_16U_5406_1.53 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-220769 was assigned to this vulnerability. **CVE ID : CVE-2023-0808**	N/A	H-BOS-INVE-270223/1399
Vendor: Cisco					
Product: 807_industrial_integrated_services_router					
Affected Version(s): -					
Improper Neutralization of Special Elements	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote	https://sec.cloudapps.cisco.com/security/center/content/Cisc	H-CIS-807_-270223/1400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	oSecurityAdvisory/cisco-sa-iox-8whGn5dL	
Product: 809_industrial_integrated_services_router					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	H-CIS-809_-270223/1401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Product: 829_industrial_integrated_services_router					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	H-CIS-829_-270223/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Product: cgr1000					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	H-CIS-CGR1-270223/1403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20076		
Product: cgr1240					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	H-CIS-CGR1-270223/1404
Product: ic3000_industrial_compute_gateway					
Affected Version(s): * Up to (excluding) 1.4.2					
Improper Neutralization of Special	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an	https://sec.cloudapps.cisco.com/security/center/	H-CIS-IC30-270223/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	
Product: ir510_wpan					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	H-CIS-IR51-270223/1406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Vendor: contec					
Product: solarview_compact					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Feb-2023	9.8	There is a command injection vulnerability in SolarView Compact through 6.00, attackers can execute commands by bypassing internal restrictions through downloader.php. **CVE ID : CVE-2023-23333**	N/A	H-CON-SOLA-270223/1407
Vendor: controlbyweb					
Product: x-400					
Affected Version(s): -					
Improper Neutralization of Input During Web Page	13-Feb-2023	6.1	Control By Web X-400 devices are vulnerable to a cross-site scripting attack, which could result in private and session information	N/A	H-CON-X-40-270223/1408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			being transferred to the attacker. **CVE ID : CVE-2023-23553**		
Product: x-600m					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Control By Web X-600M devices run Lua scripts and are vulnerable to code injection, which could allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2023-23551**	N/A	H-CON-X-60-270223/1409
Vendor: D-link					
Product: dir-605l					
Affected Version(s): -					
Out-of-bounds Write	10-Feb-2023	9.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the curTime parameter at /goform/formSetACLFilter. **CVE ID : CVE-2023-24348**	https://www.dlink.com/en/security-bulletin/	H-D-L-DIR--270223/1410
Out-of-bounds Write	10-Feb-2023	9.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the curTime parameter at /goform/formSetRoute. **CVE ID : CVE-2023-24349**	https://www.dlink.com/en/security-bulletin/	H-D-L-DIR--270223/1411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-Feb-2023	9.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the config.smtp_email_subject parameter at /goform/formSetEmail. **CVE ID : CVE-2023-24350**	https://www.dlink.com/en/security-bulletin/	H-D-L-DIR--270223/1412
Out-of-bounds Write	10-Feb-2023	9.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the FILECODE parameter at /goform/formLogin. **CVE ID : CVE-2023-24351**	https://www.dlink.com/en/security-bulletin/	H-D-L-DIR--270223/1413
Out-of-bounds Write	10-Feb-2023	9.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the webpage parameter at /goform/formWPS. **CVE ID : CVE-2023-24352**	https://www.dlink.com/en/security-bulletin/	H-D-L-DIR--270223/1414
Out-of-bounds Write	10-Feb-2023	8.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the curTime parameter at /goform/formSchedule. **CVE ID : CVE-2023-24343**	https://www.dlink.com/en/security-bulletin/	H-D-L-DIR--270223/1415
Out-of-bounds Write	10-Feb-2023	8.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a	https://www.dlink.com/en/security-bulletin/	H-D-L-DIR--270223/1416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stack overflow via the webpage parameter at /goform/formWlanGuestSetup. **CVE ID : CVE-2023-24344**		
Out-of-bounds Write	10-Feb-2023	8.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the curTime parameter at /goform/formSetWanDhcpplus. **CVE ID : CVE-2023-24345**	https://www.dlink.com/en/security-bulletin/	H-D-L-DIR--270223/1417
Out-of-bounds Write	10-Feb-2023	8.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the wan_connected parameter at /goform/formEasySetupWizard3. **CVE ID : CVE-2023-24346**	https://www.dlink.com/en/security-bulletin/	H-D-L-DIR--270223/1418
Out-of-bounds Write	10-Feb-2023	8.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the webpage parameter at /goform/formSetWanDhcpplus. **CVE ID : CVE-2023-24347**	https://www.dlink.com/en/security-bulletin/	H-D-L-DIR--270223/1419
Product: dwl-2600ap					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Feb-2023	7.8	A command injection vulnerability in the firmware_update command, in the device's restricted telnet interface, allows an authenticated attacker to execute arbitrary commands as root. **CVE ID : CVE-2023-0127**	N/A	H-D-L-DWL--270223/1420
Vendor: deyeinverter					
Product: inverter					
Affected Version(s): -					
Use of Hard-coded Credentials	13-Feb-2023	6.8	A vulnerability was found in Deye/Revolt/Bosswerk Inverter MW3_15U_5406_1.47/ MW3_15U_5406_1.471. It has been rated as problematic. This issue affects some unknown processing of the component Access Point Setting Handler. The manipulation with the input 12345678 leads to use of hard-coded password. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. Upgrading to version MW3_16U_5406_1.53 is able to address this issue. It is recommended to upgrade the affected	N/A	H-DEY-INVE-270223/1421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component. The identifier VDB-220769 was assigned to this vulnerability. **CVE ID : CVE-2023-0808**		
Vendor: F5					
Product: big-ip_10000s					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1422
Product: big-ip_10200v					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x,	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: big-ip_10200v-ssl					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22839		
Product: big-ip_12000					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1425
Product: big-ip_5000s					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: big-ip_5200v					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1427
Product: big-ip_5200v-ssl					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1428
Product: big-ip_7000s					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note:	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: big-ip_7200v					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1430
Product: big-ip_7200v-ssl					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x,	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: big-ip_i10600					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22839		
Product: big-ip_i10800					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1433
Product: big-ip_i11600					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: big-ip_i11800					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1435
Product: big-ip_i15600					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1436
Product: big-ip_i15800					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note:	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: big-ip_i5600					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1438
Product: big-ip_i5800					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x,	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: big-ip_i7600					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22839		
Product: big-ip_i7800					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-BIG--270223/1441
Product: r10600					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies	https://my.f5.com/manage/s/article/K37708118	H-F5-R106-270223/1442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: r10800					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-R108-270223/1443
Product: r10900					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-R109-270223/1444
Product: r5600					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note:	https://my.f5.com/manage/s/article/K37708118	H-F5-R560-270223/1445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: r5800					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-R580-270223/1446
Product: r5900					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x,	https://my.f5.com/manage/s/article/K37708118	H-F5-R590-270223/1447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: velos_bx110					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K37708118	H-F5-VELO-270223/1448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22839		
Product: viprion_b2100					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-VIPR-270223/1449
Product: viprion_b2150					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies	https://my.f5.com/manage/s/article/K37708118	H-F5-VIPR-270223/1450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: viprion_b2250					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-VIPR-270223/1451
Product: viprion_b4300					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	H-F5-VIPR-270223/1452
Product: viprion_b4450					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note:	https://my.f5.com/manage/s/article/K37708118	H-F5-VIPR-270223/1453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Vendor: ls-electric					
Product: xbc-dn32u					
Affected Version(s): -					
Missing Authentication for Critical Function	15-Feb-2023	9.8	LS ELECTRIC XBC-DN32U with operating system version 01.80 is missing authentication to create users on the PLC. This could allow an attacker to create and use an account with elevated privileges and take control of the device. **CVE ID : CVE-2023-22804**	N/A	H-LS--XBC--270223/1454
N/A	15-Feb-2023	9.8	LS ELECTRIC XBC-DN32U with operating system version 01.80 does not properly control access to the PLC over its internal XGT protocol. An attacker could control and tamper with the PLC by sending the packets to the PLC over its XGT protocol. **CVE ID : CVE-2023-22807**	N/A	H-LS--XBC--270223/1455
Missing Authentication for	15-Feb-2023	9.1	LS ELECTRIC XBC-DN32U with operating system version 01.80 is missing authentication	N/A	H-LS--XBC--270223/1456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			for its deletion command. This could allow an attacker to delete arbitrary files. **CVE ID : CVE-2023-0102**		
Access of Memory Location After End of Buffer	15-Feb-2023	7.5	If an attacker were to access memory locations of LS ELECTRIC XBC-DN32U with operating system version 01.80 that are outside of the communication buffer, the device stops operating. This could allow an attacker to cause a denial-of-service condition. **CVE ID : CVE-2023-0103**	N/A	H-LS--XBC--270223/1457
Missing Authentication for Critical Function	15-Feb-2023	7.5	LS ELECTRIC XBC-DN32U with operating system version 01.80 is missing authentication to perform critical functions to the PLC. This could allow an attacker to change the PLC's mode arbitrarily. **CVE ID : CVE-2023-22803**	N/A	H-LS--XBC--270223/1458
Cleartext Transmission of Sensitive Information	15-Feb-2023	7.5	LS ELECTRIC XBC-DN32U with operating system version 01.80 transmits sensitive information in cleartext when communicating over its XGT protocol. This could allow an attacker to gain sensitive information	N/A	H-LS--XBC--270223/1459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such as user credentials. **CVE ID : CVE-2023-22806**		
N/A	15-Feb-2023	4.3	LS ELECTRIC XBC-DN32U with operating system version 01.80 has improper access control to its read prohibition feature. This could allow a remote attacker to remotely set the feature to lock users out of reading data from the device. **CVE ID : CVE-2023-22805**	N/A	H-LS--XBC--270223/1460
Vendor: mediatek					
Product: mt6580					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT65-270223/1461
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege	https://corp.mediatek.com/product-security-	H-MED-MT65-270223/1462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	bulletin/February-2023	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT65-270223/1463
Product: mt6731					
Affected Version(s): -					
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1465
Product: mt6735					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1466
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1468
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1469
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**		
Product: mt6737					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1471
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1472
Access of Resource	06-Feb-2023	6.7	In ion, there is a possible out of bounds	https://corp.mediatek.co	H-MED-MT67-270223/1473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Using Incompatible Type ('Type Confusion')			read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	m/product-security-bulletin/February-2023	
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1474
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt6739					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1476
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1477
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**		
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1479
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1480
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1482
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1483
Improper Restriction of Operations within the	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT67-270223/1484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	bulletin/February-2023	
Product: mt6753					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1485
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20604		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1487
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1488
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**		
Product: mt6757					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1490
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1491
Access of Resource Using Incompatible Type	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT67-270223/1492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	bulletin/February-2023	
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1493
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1494
Product: mt6757c					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1495
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1496
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20605		
Product: mt6757cd					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1498
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1499
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**		
Product: mt6757ch					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1501
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1502
Improper Restriction of Operations	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT67-270223/1503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	bulletin/February-2023	
Product: mt6761					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1504
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20604		
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1506
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1507
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1509
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1510
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**		
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1512
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1513
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT67-270223/1514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	bulletin/February-2023	
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1515
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1516
Product: mt6762					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1517
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1518
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1520
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1521
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**		
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1523
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1524
Improper Restriction of Operations within the Bounds of	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**		
Product: mt6763					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1526
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1528
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1529
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20605		
Product: mt6765					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1531
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1532
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**		
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1534
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1535
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-	H-MED-MT67-270223/1536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	bulletin/February-2023	
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1537
Improper Synchronization	06-Feb-2023	6.4	In ccu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07512839; Issue ID: ALPS07512839. **CVE ID : CVE-2023-20607**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1538
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free	https://corp.mediatek.co	H-MED-MT67-270223/1539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	m/product-security-bulletin/February-2023	
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1540
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1542
Product: mt6768					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1543
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**		
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1545
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1546
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1548
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1549
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This	https://corp.mediatek.com/product-security-	H-MED-MT67-270223/1550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	bulletin/February-2023	
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1551
Improper Synchronization	06-Feb-2023	6.4	In ccu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07512839; Issue ID: ALPS07512839. **CVE ID : CVE-2023-20607**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1553
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1554
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20611		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1556
Product: mt6769					
Affected Version(s): -					
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1557
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1559
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1560
Access of Resource Using Incompatible Type	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT67-270223/1561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	bulletin/February-2023	
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1562
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1564
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1565
Product: mt6771					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**		
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1567
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1568
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1570
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1571
Access of Resource Using Incompatible Type	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT67-270223/1572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	bulletin/February-2023	
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1573
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1574
Product: mt6779					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1575
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1576
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**		
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1578
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1579
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1581
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1582
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT67-270223/1583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	bulletin/February-2023	
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1584
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1585
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition.	https://corp.mediatek.com/product-	H-MED-MT67-270223/1586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	security-bulletin/February-2023	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1587
Product: mt6781					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20602		
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1589
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1590
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1592
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1593
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**		
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1595
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1596
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT67-270223/1597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	bulletin/February-2023	
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1598
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1599
Improper Restriction of	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing	https://corp.mediatek.com/product-	H-MED-MT67-270223/1600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	security-bulletin/February-2023	
Product: mt6785					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1601
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20604		
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1603
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1604
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1606
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1607
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**		
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1609
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1610
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT67-270223/1611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	bulletin/February-2023	
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1612
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1613
Product: mt6789					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1614
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1615
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1617
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1618
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**		
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1620
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1621
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT67-270223/1623
Product: mt6833					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1625
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1626
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1628
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1629
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**		
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1631
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1632
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege	https://corp.mediatek.com/product-security-	H-MED-MT68-270223/1633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	bulletin/February-2023	
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1634
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1635
Improper Restriction of Operations	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT68-270223/1636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	bulletin/February-2023	
Out-of-bounds Read	06-Feb-2023	4.4	In ccu, there is a possible out of bounds read due to a logic error. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570864; Issue ID: ALPS07570864. **CVE ID : CVE-2023-20609**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1637
Product: mt6853					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20602		
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1639
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1640
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1642
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1643
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**		
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1645
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1646
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT68-270223/1647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	bulletin/February-2023	
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1648
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1649
Improper Restriction of	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing	https://corp.mediatek.com/product-	H-MED-MT68-270223/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	security-bulletin/February-2023	
Out-of-bounds Read	06-Feb-2023	4.4	In ccu, there is a possible out of bounds read due to a logic error. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570864; Issue ID: ALPS07570864. **CVE ID : CVE-2023-20609**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1651
Product: mt6853t					
Affected Version(s): -					
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20614		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1653
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1654
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**		
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1656
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1657
Product: mt6855					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT68-270223/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	bulletin/February-2023	
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1659
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1661
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1662
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1664
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1665
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1667
Product: mt6873					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1668
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT68-270223/1669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	bulletin/February-2023	
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1670
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1672
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1673
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**		
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1675
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1676
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**		
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1678
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1679
Improper Restriction of Operations within the Bounds of	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**		
Out-of-bounds Read	06-Feb-2023	4.4	In ccu, there is a possible out of bounds read due to a logic error. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570864; Issue ID: ALPS07570864. **CVE ID : CVE-2023-20609**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1681
Product: mt6875					
Affected Version(s): -					
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1683
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1684
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1686
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1687
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**		
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1689
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1690
Product: mt6877					
Affected Version(s): -					
Integer Overflow or	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer	https://corp.mediatek.com/product-	H-MED-MT68-270223/1691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	security-bulletin/February-2023	
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1692
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1694
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1695
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1697
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1698
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**		
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1700
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1701
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1703
Out-of-bounds Read	06-Feb-2023	4.4	In ccu, there is a possible out of bounds read due to a logic error. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570864; Issue ID: ALPS07570864. **CVE ID : CVE-2023-20609**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1704
Product: mt6879					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1705
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1706
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**		
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1708
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1709
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1711
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1712
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1714
Improper Input Validation	06-Feb-2023	4.4	In apusys, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571104; Issue ID: ALPS07571104. **CVE ID : CVE-2023-20606**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1715
Product: mt6883					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1716
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1717
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1719
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1720
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**		
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1722
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1723
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**		
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1725
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1726
Product: mt6885					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1727
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1728
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**		
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1730
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1731
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1733
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1734
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT68-270223/1735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	bulletin/February-2023	
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1736
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1737
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition.	https://corp.mediatek.com/product-	H-MED-MT68-270223/1738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	security-bulletin/February-2023	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1739
Out-of-bounds Read	06-Feb-2023	4.4	In ccu, there is a possible out of bounds read due to a logic error. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570864; Issue ID: ALPS07570864. **CVE ID : CVE-2023-20609**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1740
Product: mt6889					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1741
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1742
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**		
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1744
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1745
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1747
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1748
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT68-270223/1749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	bulletin/February-2023	
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1750
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1751
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition.	https://corp.mediatek.com/product-	H-MED-MT68-270223/1752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	security-bulletin/February-2023	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1753
Product: mt6891					
Affected Version(s): -					
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20612		
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1755
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1756
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1758
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1759
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**		
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1761
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1762
Product: mt6893					
Affected Version(s): -					
Integer Overflow	06-Feb-2023	6.7	In ged, there is a possible out of bounds	https://corp.mediatek.co	H-MED-MT68-270223/1763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	m/product-security-bulletin/February-2023	
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1764
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20612		
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1766
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1767
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1769
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1770
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**		
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1772
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1773
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege	https://corp.mediatek.com/product-security-	H-MED-MT68-270223/1774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	bulletin/February-2023	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1775
Out-of-bounds Read	06-Feb-2023	4.4	In ccu, there is a possible out of bounds read due to a logic error. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570864; Issue ID: ALPS07570864. **CVE ID : CVE-2023-20609**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1776
Product: mt6895					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1777
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1778
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**		
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1780
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1781
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1783
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1784
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1786
Improper Input Validation	06-Feb-2023	4.4	In apusys, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571104; Issue ID: ALPS07571104. **CVE ID : CVE-2023-20606**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT68-270223/1787
Product: mt6983					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT69-270223/1788
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT69-270223/1789
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT69-270223/1790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**		
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT69-270223/1791
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT69-270223/1792
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT69-270223/1793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT69-270223/1794
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT69-270223/1795
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT69-270223/1796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT69-270223/1797
Improper Input Validation	06-Feb-2023	4.4	In apusys, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571104; Issue ID: ALPS07571104. **CVE ID : CVE-2023-20606**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT69-270223/1798
Product: mt8167					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT81-270223/1799
Product: mt8168					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT81-270223/1800
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT81-270223/1801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**		
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT81-270223/1802
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT81-270223/1803
Product: mt8183					
Affected Version(s): -					
Access of Resource Using Incompatible Type	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT81-270223/1804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**		
Product: mt8185					
Affected Version(s): -					
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT81-270223/1805
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT81-270223/1806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT81-270223/1807
Product: mt8321					
Affected Version(s): -					
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1808
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1810
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1811
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1813
Product: mt8362a					
Affected Version(s): -					
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1814
Product: mt8365					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1815
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1816
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**		
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1818
Product: mt8385					
Affected Version(s): -					
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1819
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1821
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1822
Access of Resource Using	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type	https://corp.mediatek.com/product-	H-MED-MT83-270223/1823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incompatible Type ('Type Confusion')			confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	security-bulletin/February-2023	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT83-270223/1824
Product: mt8666					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT86-270223/1825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20616		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT86-270223/1826
Product: mt8667					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT86-270223/1827
Product: mt8675					
Affected Version(s): -					
Access of Resource Using Incompatible Type	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT86-270223/1828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	bulletin/February-2023	
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT86-270223/1829
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT86-270223/1830
Product: mt8765					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1831
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1832
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1834
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1835
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**		
Product: mt8766					
Affected Version(s): -					
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1837
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1839
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1840
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1842
Product: mt8768					
Affected Version(s): -					
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1843
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-	H-MED-MT87-270223/1844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	bulletin/February-2023	
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1845
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1846
Access of Resource	06-Feb-2023	6.7	In ion, there is a possible out of bounds	https://corp.mediatek.co	H-MED-MT87-270223/1847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Using Incompatible Type ('Type Confusion')			read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	m/product-security-bulletin/February-2023	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1848
Out-of-bounds Read	06-Feb-2023	4.4	In ccu, there is a possible out of bounds read due to a logic error. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570864; Issue ID: ALPS07570864.	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20609		
Product: mt8786					
Affected Version(s): -					
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1850
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1851
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1853
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1854
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT87-270223/1855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	bulletin/February-2023	
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1856
Improper Synchronization	06-Feb-2023	6.4	In ccu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07512839; Issue ID: ALPS07512839. **CVE ID : CVE-2023-20607**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1857
Improper Restriction	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds	https://corp.mediatek.co	H-MED-MT87-270223/1858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	m/product-security-bulletin/February-2023	
Out-of-bounds Read	06-Feb-2023	4.4	In ccu, there is a possible out of bounds read due to a logic error. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570864; Issue ID: ALPS07570864. **CVE ID : CVE-2023-20609**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1859
Product: mt8788					
Affected Version(s): -					
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**		
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1861
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1862
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1864
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1865
Product: mt8789					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1866
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1867
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1869
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1870
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1872
Product: mt8791					
Affected Version(s): -					
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1874
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1875
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1877
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1878
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**		
Out-of-bounds Read	06-Feb-2023	4.4	In ccu, there is a possible out of bounds read due to a logic error. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570864; Issue ID: ALPS07570864. **CVE ID : CVE-2023-20609**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1880
Product: mt8791t					
Affected Version(s): -					
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1882
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1883
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1885
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1886
Product: mt8797					
Affected Version(s): -					
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-	H-MED-MT87-270223/1887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	bulletin/February-2023	
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1888
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1890
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1891
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**		
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1893
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1894
Out-of-bounds Read	06-Feb-2023	4.4	In ccu, there is a possible out of bounds read due to a logic error. This could lead to local information disclosure with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	H-MED-MT87-270223/1895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07570864; Issue ID: ALPS07570864. **CVE ID : CVE-2023-20609**		
Vendor: multilaser					
Product: re057					
Affected Version(s): -					
N/A	03-Feb-2023	7.5	A vulnerability, which was classified as critical, was found in Multilaser RE057 and RE170 2.1/2.2. This affects an unknown part of the file /param.file.tgz of the component Backup File Handler. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The identifier VDB-220053 was assigned to this vulnerability. **CVE ID : CVE-2023-0658**	N/A	H-MUL-RE05-270223/1896
Product: re170					
Affected Version(s): -					
N/A	03-Feb-2023	7.5	A vulnerability, which was classified as critical, was found in Multilaser RE057 and RE170 2.1/2.2. This affects an unknown part of the file /param.file.tgz of the component Backup File Handler. The	N/A	H-MUL-RE17-270223/1897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation leads to information disclosure. It is possible to initiate the attack remotely. The identifier VDB-220053 was assigned to this vulnerability. **CVE ID : CVE-2023-0658**		
Vendor: Netgear					
Product: d6100					
Affected Version(s): -					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and	https://www.netgear.com/about/security/	H-NET-D610-270223/1898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier. **CVE ID : CVE-2023-23110**		
Product: dgn1000v3					
Affected Version(s): -					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500	https://www.netgear.com/about/security/	H-NET-DGN1-270223/1899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier. **CVE ID : CVE-2023-23110**		
Product: prosafe_fs726tp					
Affected Version(s): -					
Insufficiently Protected Credentials	15-Feb-2023	7.5	An uspecified endpoint in the web server of the switch does not properly authenticate the user identity, and may allow downloading a config page with the password to the switch in clear text. **CVE ID : CVE-2023-24498**	N/A	H-NET-PROS-270223/1900
Product: r8900					
Affected Version(s): -					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless	https://www.netgear.com/about/security/	H-NET-R890-270223/1901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier. **CVE ID : CVE-2023-23110**		
Product: r9000					
Affected Version(s): -					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and	https://www.netgear.com/about/security/	H-NET-R900-270223/1902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier. **CVE ID : CVE-2023-23110**		
Product: wndr3700					
Affected Version(s): v2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	15-Feb-2023	9.8	A vulnerability has been found in Netgear WNDR3700v2 1.0.1.14 and classified as critical. This vulnerability affects unknown code of the component Web Interface. The manipulation leads to command injection. 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-221152.	N/A	H-NET-WNDR-270223/1903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0849		
N/A	15-Feb-2023	7.5	A vulnerability was found in Netgear WNDR3700v2 1.0.1.14. It has been rated as problematic. This issue affects some unknown processing of the component Web Management Interface. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221147. **CVE ID : CVE-2023-0848**	N/A	H-NET-WNDR-270223/1904
N/A	15-Feb-2023	7.5	A vulnerability was found in Netgear WNDR3700v2 1.0.1.14 and classified as problematic. This issue affects some unknown processing of the component Web Interface. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221153 was assigned to this vulnerability.	N/A	H-NET-WNDR-270223/1905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0850		
Product: wnr1000v2					
Affected Version(s): -					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier.	https://www.netgear.com/about/security/	H-NET-WNR1-270223/1906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23110		
Product: wnr2200					
Affected Version(s): -					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier.	https://www.netgear.com/about/security/	H-NET-WNR2-270223/1907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23110		
Product: wnr2500					
Affected Version(s): -					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier.	https://www.netgear.com/about/security/	H-NET-WNR2-270223/1908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23110		
Product: wnr612v2					
Affected Version(s): -					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier.	https://www.netgear.com/about/security/	H-NET-WNR6-270223/1909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23110		
Product: xavn2001v2					
Affected Version(s): -					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier.	https://www.netgear.com/about/security/	H-NET-XAVN-270223/1910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23110		
Vendor: onekey					
Product: onekey_mini					
Affected Version(s): -					
N/A	14-Feb-2023	4.2	Onekey Touch devices through 4.0.0 and Onekey Mini devices through 2.10.0 allow man-in-the-middle attackers to obtain the seed phase. The man-in-the-middle access can only be obtained after disassembling a device (i.e., here, "man-in-the-middle" does not refer to the attacker's position on an IP network). NOTE: the vendor states that "our hardware team has updated the security patch without anyone being affected." **CVE ID : CVE-2023-25758**	https://blog.onekey.so/our-response-to-recent-security-fix-reports-13914fea8afd	H-ONE-ONEK-270223/1911
Product: onekey_touch					
Affected Version(s): -					
N/A	14-Feb-2023	4.2	Onekey Touch devices through 4.0.0 and Onekey Mini devices through 2.10.0 allow man-in-the-middle attackers to obtain the seed phase. The man-in-the-middle access can only be obtained after disassembling a device (i.e., here, "man-in-the-middle" does not	https://blog.onekey.so/our-response-to-recent-security-fix-reports-13914fea8afd	H-ONE-ONEK-270223/1912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			refer to the attacker's position on an IP network). NOTE: the vendor states that "our hardware team has updated the security patch without anyone being affected." **CVE ID : CVE-2023-25758**		
Vendor: Planex					
Product: cs-wmv02g					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	14-Feb-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** Cross-site request forgery (CSRF) vulnerability in Wired/Wireless LAN Pan/Tilt Network Camera CS-WMV02G all versions allows a remote unauthenticated attacker to hijack the authentication and conduct arbitrary operations by having a logged-in user to view a malicious page. NOTE: This vulnerability only affects products that are no longer supported by the developer. **CVE ID : CVE-2023-22375**	N/A	H-PLA-CS-W-270223/1913
Improper Neutralization of Input During Web Page Generation	14-Feb-2023	6.1	** UNSUPPORTED WHEN ASSIGNED ** Reflected cross-site scripting vulnerability in Wired/Wireless LAN Pan/Tilt Network Camera CS-WMV02G all	N/A	H-PLA-CS-W-270223/1914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			versions allows a remote unauthenticated attacker to inject arbitrary script to inject an arbitrary script. NOTE: This vulnerability only affects products that are no longer supported by the developer. **CVE ID : CVE-2023-22376**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.2	** UNSUPPORTED WHEN ASSIGNED ** Stored cross-site scripting vulnerability in Wired/Wireless LAN Pan/Tilt Network Camera CS-WMV02G all versions allows a network-adjacent authenticated attacker to inject an arbitrary script. NOTE: This vulnerability only affects products that are no longer supported by the developer. **CVE ID : CVE-2023-22370**	https://www.planex.co.jp/support/support_end_list.shtml	H-PLA-CS-W-270223/1915
Vendor: revolt-power					
Product: inverter					
Affected Version(s): -					
Use of Hard-coded Credentials	13-Feb-2023	6.8	A vulnerability was found in Deye/Revolt/Bosswerk Inverter MW3_15U_5406_1.47/ MW3_15U_5406_1.471. It has been rated as problematic. This issue affects some unknown	N/A	H-REV-INVE-270223/1916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing of the component Access Point Setting Handler. The manipulation with the input 12345678 leads to use of hard-coded password. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. Upgrading to version MW3_16U_5406_1.53 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-220769 was assigned to this vulnerability. **CVE ID : CVE-2023-0808**		
Vendor: Ruckuswireless					
Product: e510					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-E510-270223/1917
Product: h320					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-H320-270223/1918
Product: h350					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-H350-270223/1919
Product: h500					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-H500-270223/1920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: h510					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-H510-270223/1921
Product: h550					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-H550-270223/1922
Product: m510					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring.	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-M510-270223/1923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25717		
Product: m510-jp					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-M510-270223/1924
Product: p300					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-P300-270223/1925
Product: q410					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&pass	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-Q410-270223/1926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			word=password$(curl substring. **CVE ID : CVE-2023-25717**		
Product: q710					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-Q710-270223/1927
Product: q910					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-Q910-270223/1928
Product: r300					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R300-270223/1929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**		
Product: r310					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R310-270223/1930
Product: r320					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R320-270223/1931
Product: r350					
Affected Version(s): -					
Improper Control of Generation of Code	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated	https://support.ruckuswireless.com/s	H-RUC-R350-270223/1932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	ecurity_bulletins/315	
Product: r500					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R500-270223/1933
Product: r510					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R510-270223/1934
Product: r550					
Affected Version(s): -					
Improper Control of	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows	https://support.ruckuswi	H-RUC-R550-270223/1935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	reless.com/security_bulletins/315	
Product: r560					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R560-270223/1936
Product: r600					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R600-270223/1937
Product: r610					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R610-270223/1938
Product: r650					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R650-270223/1939
Product: r700					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R700-270223/1940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: r710					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R710-270223/1941
Product: r720					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R720-270223/1942
Product: r730					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring.	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R730-270223/1943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25717		
Product: r750					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R750-270223/1944
Product: r760					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R760-270223/1945
Product: r850					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&pass	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-R850-270223/1946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			word=password$(curl substring. **CVE ID : CVE-2023-25717**		
Product: sz-144					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-SZ-1-270223/1947
Product: sz-144-federal					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-SZ-1-270223/1948
Product: sz100					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-SZ10-270223/1949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**		
Product: sz300					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-SZ30-270223/1950
Product: sz300-federal					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-SZ30-270223/1951
Product: t300					
Affected Version(s): -					
Improper Control of Generation of Code	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated	https://support.ruckuswireless.com/s	H-RUC-T300-270223/1952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	ecurity_bulletins/315	
Product: t301n					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T301-270223/1953
Product: t301s					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T301-270223/1954
Product: t310c					
Affected Version(s): -					
Improper Control of	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows	https://support.ruckuswi	H-RUC-T310-270223/1955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	reless.com/security_bulletins/315	
Product: t310d					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T310-270223/1956
Product: t310n					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T310-270223/1957
Product: t310s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T310-270223/1958
Product: t350c					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T350-270223/1959
Product: t350d					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T350-270223/1960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: t350se					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T350-270223/1961
Product: t504					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T504-270223/1962
Product: t610					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring.	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T610-270223/1963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25717		
Product: t710					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T710-270223/1964
Product: t710s					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T710-270223/1965
Product: t750					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&pass	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T750-270223/1966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			word=password$(curl substring. **CVE ID : CVE-2023-25717**		
Product: t750se					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T750-270223/1967
Product: t811-cm					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T811-270223/1968
Product: t811-cm\(non-spf\)					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-T811-270223/1969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**		
Product: zd1000					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-ZD10-270223/1970
Product: zd1100					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-ZD11-270223/1971
Product: zd1200					
Affected Version(s): -					
Improper Control of Generation of Code	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated	https://support.ruckuswireless.com/s	H-RUC-ZD12-270223/1972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	ecurity_bulletins/315	
Product: zd3000					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-ZD30-270223/1973
Product: zd5000					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	H-RUC-ZD50-270223/1974
Vendor: sunellsecurity					
Product: sn-adr3804e1					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	15-Feb-2023	7.5	Sunell DVR, latest version, Insufficiently Protected Credentials (CWE-522) may be exposed through an unspecified request. **CVE ID : CVE-2023-23463**	N/A	H-SUN-SN-A-270223/1975
N/A	15-Feb-2023	6.5	Sunell DVR, latest version, CWE-200: Exposure of Sensitive Information to an Unauthorized Actor through an unspecified request. **CVE ID : CVE-2023-23458**	N/A	H-SUN-SN-A-270223/1976
Product: sn-adr3808e1					
Affected Version(s): -					
Insufficiently Protected Credentials	15-Feb-2023	7.5	Sunell DVR, latest version, Insufficiently Protected Credentials (CWE-522) may be exposed through an unspecified request. **CVE ID : CVE-2023-23463**	N/A	H-SUN-SN-A-270223/1977
N/A	15-Feb-2023	6.5	Sunell DVR, latest version, CWE-200: Exposure of Sensitive Information to an Unauthorized Actor through an unspecified request. **CVE ID : CVE-2023-23458**	N/A	H-SUN-SN-A-270223/1978
Product: sn-adr3808e2					
Affected Version(s): -					
Insufficiently	15-Feb-2023	7.5	Sunell DVR, latest version, Insufficiently	N/A	H-SUN-SN-A-270223/1979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Protected Credentials (CWE-522) may be exposed through an unspecified request. **CVE ID : CVE-2023-23463**		
N/A	15-Feb-2023	6.5	Sunell DVR, latest version, CWE-200: Exposure of Sensitive Information to an Unauthorized Actor through an unspecified request. **CVE ID : CVE-2023-23458**	N/A	H-SUN-SN-A-270223/1980
Product: sn-adr3816e1					
Affected Version(s): -					
Insufficiently Protected Credentials	15-Feb-2023	7.5	Sunell DVR, latest version, Insufficiently Protected Credentials (CWE-522) may be exposed through an unspecified request. **CVE ID : CVE-2023-23463**	N/A	H-SUN-SN-A-270223/1981
N/A	15-Feb-2023	6.5	Sunell DVR, latest version, CWE-200: Exposure of Sensitive Information to an Unauthorized Actor through an unspecified request. **CVE ID : CVE-2023-23458**	N/A	H-SUN-SN-A-270223/1982
Product: sn-adr3816e2					
Affected Version(s): -					
Insufficiently Protected Credentials	15-Feb-2023	7.5	Sunell DVR, latest version, Insufficiently Protected Credentials (CWE-522) may be	N/A	H-SUN-SN-A-270223/1983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exposed through an unspecified request. **CVE ID : CVE-2023-23463**		
N/A	15-Feb-2023	6.5	Sunell DVR, latest version, CWE-200: Exposure of Sensitive Information to an Unauthorized Actor through an unspecified request. **CVE ID : CVE-2023-23458**	N/A	H-SUN-SN-A-270223/1984
Product: sn-xvr3804e1					
Affected Version(s): -					
Insufficiently Protected Credentials	15-Feb-2023	7.5	Sunell DVR, latest version, Insufficiently Protected Credentials (CWE-522) may be exposed through an unspecified request. **CVE ID : CVE-2023-23463**	N/A	H-SUN-SN-X-270223/1985
N/A	15-Feb-2023	6.5	Sunell DVR, latest version, CWE-200: Exposure of Sensitive Information to an Unauthorized Actor through an unspecified request. **CVE ID : CVE-2023-23458**	N/A	H-SUN-SN-X-270223/1986
Product: sn-xvr3808e2					
Affected Version(s): -					
Insufficiently Protected Credentials	15-Feb-2023	7.5	Sunell DVR, latest version, Insufficiently Protected Credentials (CWE-522) may be exposed through an unspecified request.	N/A	H-SUN-SN-X-270223/1987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23463		
N/A	15-Feb-2023	6.5	Sunell DVR, latest version, CWE-200: Exposure of Sensitive Information to an Unauthorized Actor through an unspecified request. **CVE ID : CVE-2023-23458**	N/A	H-SUN-SN-X-270223/1988
Vendor: Tenda					
Product: ac23					
Affected Version(s): -					
Out-of-bounds Write	11-Feb-2023	9.8	A vulnerability was found in Tenda AC23 16.03.07.45 and classified as critical. Affected by this issue is the function formSetSysToolDDNS/formGetSysToolDDNS of the file /bin/httpd. The manipulation leads to out-of-bounds write. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-220640. **CVE ID : CVE-2023-0782**	N/A	H-TEN-AC23-270223/1989
Vendor: totolink					
Product: a7100ru					
Affected Version(s): -					
Improper Neutralizat	06-Feb-2023	9.8	TOTOlink A7100RU(V7.4cu.2313_	N/A	H-TOT-A710-270223/1990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			B20191024) was discovered to contain a command injection vulnerability via the country parameter at setting/delStaticDhcpRules. **CVE ID : CVE-2023-24276**		
Product: ca300-poe					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the host_time parameter in the NTPSyncWithHost function. **CVE ID : CVE-2023-24138**	N/A	H-TOT-CA30-270223/1991
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the NetDiagHost parameter in the setNetworkDiag function. **CVE ID : CVE-2023-24139**	N/A	H-TOT-CA30-270223/1992
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the NetDiagPingNum parameter in the setNetworkDiag function.	N/A	H-TOT-CA30-270223/1993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24140		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the NetDiagPingTimeOut parameter in the setNetworkDiag function. **CVE ID : CVE-2023-24141**	N/A	H-TOT-CA30-270223/1994
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the NetDiagPingSize parameter in the setNetworkDiag function. **CVE ID : CVE-2023-24142**	N/A	H-TOT-CA30-270223/1995
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the NetDiagTracertHop parameter in the setNetworkDiag function. **CVE ID : CVE-2023-24143**	N/A	H-TOT-CA30-270223/1996
Improper Neutralization of Special Elements used in a Command	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the hour parameter in the	N/A	H-TOT-CA30-270223/1997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			setRebootScheCfg function. **CVE ID : CVE-2023-24144**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the plugin_version parameter in the setUnloadUserData function. **CVE ID : CVE-2023-24145**	N/A	H-TOT-CA30-270223/1998
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the minute parameter in the setRebootScheCfg function. **CVE ID : CVE-2023-24146**	N/A	H-TOT-CA30-270223/1999
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the FileName parameter in the setUploadUserData function. **CVE ID : CVE-2023-24148**	N/A	H-TOT-CA30-270223/2000
Use of Hard-coded Credentials	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a hard code password for root which is stored in	N/A	H-TOT-CA30-270223/2001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the component /etc/shadow. **CVE ID : CVE-2023-24149**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	14-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the admpass parameter in the setPasswordCfg function. **CVE ID : CVE-2023-24159**	N/A	H-TOT-CA30-270223/2002
Improper Neutralization of Special Elements used in a Command ('Command Injection')	14-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the admuser parameter in the setPasswordCfg function. **CVE ID : CVE-2023-24160**	N/A	H-TOT-CA30-270223/2003
Improper Neutralization of Special Elements used in a Command ('Command Injection')	14-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the webWlanIdx parameter in the setWebWlanIdx function. **CVE ID : CVE-2023-24161**	N/A	H-TOT-CA30-270223/2004
Use of Hard-coded Credentials	03-Feb-2023	7.5	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a hard code password for the telnet service which is stored in the	N/A	H-TOT-CA30-270223/2005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component /etc/config/product.ini. **CVE ID : CVE-2023-24147**		
Product: t8					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	A command injection vulnerability in the serverIp parameter in the function meshSlaveDlfw of TOTOLINK T8 V4.1.5cu allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2023-24150**	N/A	H-TOT-T8-270223/2006
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	A command injection vulnerability in the ip parameter in the function recvSlaveCloudCheckStatus of TOTOLINK T8 V4.1.5cu allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2023-24151**	N/A	H-TOT-T8-270223/2007
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	A command injection vulnerability in the serverIp parameter in the function meshSlaveUpdate of TOTOLINK T8 V4.1.5cu allows attackers to execute arbitrary commands via a crafted MQTT packet.	N/A	H-TOT-T8-270223/2008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24152		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	A command injection vulnerability in the version parameter in the function recvSlaveCloudCheckStatus of TOTOLINK T8 V4.1.5cu allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2023-24153**	N/A	H-TOT-T8-270223/2009
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK T8 V4.1.5cu was discovered to contain a command injection vulnerability via the slaveIpList parameter in the function setUpgradeFW. **CVE ID : CVE-2023-24154**	N/A	H-TOT-T8-270223/2010
Use of Hard-coded Credentials	03-Feb-2023	9.8	TOTOLINK T8 V4.1.5cu was discovered to contain a hard code password for the telnet service which is stored in the component /web_cste/cgi-bin/product.ini. **CVE ID : CVE-2023-24155**	N/A	H-TOT-T8-270223/2011
Improper Neutralization of Special Elements used in a Command ('Comman	03-Feb-2023	9.8	A command injection vulnerability in the ip parameter in the function recvSlaveUpgstatus of TOTOLINK T8 V4.1.5cu allows attackers to execute arbitrary	N/A	H-TOT-T8-270223/2012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			commands via a crafted MQTT packet. **CVE ID : CVE-2023-24156**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	A command injection vulnerability in the serverIp parameter in the function updateWifiInfo of TOTOLINK T8 V4.1.5cu allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2023-24157**	N/A	H-TOT-T8-270223/2013
Vendor: Trendnet					
Product: tew-652brp					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Feb-2023	9.8	A vulnerability was found in TRENDnet TEW-652BRP 3.04b01. It has been classified as critical. Affected is an unknown function of the file ping.ccp of the component Web Interface. The manipulation leads to command injection. 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-220020. **CVE ID : CVE-2023-0640**	N/A	H-TRE-TEW--270223/2014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Feb-2023	8.8	A vulnerability, which was classified as critical, has been found in TRENDnet TEW-652BRP 3.04B01. This issue affects some unknown processing of the file get_set.ccp of the component Web Management Interface. The manipulation leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-219935. **CVE ID : CVE-2023-0611**	N/A	H-TRE-TEW--270223/2015
Out-of-bounds Write	01-Feb-2023	7.5	A vulnerability was found in TRENDnet TEW-652BRP 3.04B01. It has been declared as critical. This vulnerability affects unknown code of the file cfg_op.ccp of the component Web Service. The manipulation leads to memory corruption. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-219958 is the identifier assigned to this vulnerability.	N/A	H-TRE-TEW--270223/2016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0618		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Feb-2023	6.1	A vulnerability was found in TRENDnet TEW-652BRP 3.04b01 and classified as problematic. This issue affects some unknown processing of the file get_set.ccp of the component Web Management Interface. The manipulation of the argument nextPage leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-220019. **CVE ID : CVE-2023-0639**	N/A	H-TRE-TEW--270223/2017
Product: tew-811dru					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Feb-2023	9.8	A vulnerability has been found in TRENDnet TEW-811DRU 1.0.10.0 and classified as critical. This vulnerability affects unknown code of the component Web Interface. The manipulation leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-220018 is	N/A	H-TRE-TEW--270223/2018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0638**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	A vulnerability, which was classified as critical, was found in TRENDnet TEW-811DRU 1.0.10.0. Affected is an unknown function of the file /wireless/basic.asp of the component httpd. The manipulation leads to 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-219936. **CVE ID : CVE-2023-0612**	N/A	H-TRE-TEW--270223/2019
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Feb-2023	7.5	A vulnerability has been found in TRENDnet TEW-811DRU 1.0.10.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /wireless/security.asp of the component httpd. The manipulation leads to memory corruption. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The	N/A	H-TRE-TEW--270223/2020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier VDB-219937 was assigned to this vulnerability. **CVE ID : CVE-2023-0613**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	A vulnerability was found in TRENDNet TEW-811DRU 1.0.10.0. It has been classified as critical. This affects an unknown part of the file /wireless/guestnetwork.asp of the component httpd. The manipulation leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-219957 was assigned to this vulnerability. **CVE ID : CVE-2023-0617**	N/A	H-TRE-TEW--270223/2021
Out-of-bounds Write	02-Feb-2023	6.5	A vulnerability, which was classified as critical, was found in TRENDnet TEW-811DRU 1.0.10.0. This affects an unknown part of the file wan.asp of the component Web Management Interface. The manipulation leads to memory corruption. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-220017	N/A	H-TRE-TEW--270223/2022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was assigned to this vulnerability. **CVE ID : CVE-2023-0637**		
Product: tv-ip651wi					
Affected Version(s): -					
Improper Validation of Integrity Check Value	02-Feb-2023	5.9	The use of the cyclic redundancy check (CRC) algorithm for integrity check during firmware update makes TRENDnet TV-IP651WI Network Camera firmware version v1.07.01 and earlier vulnerable to firmware modification attacks. An attacker can conduct a man-in-the-middle (MITM) attack to modify the new firmware image and bypass the checksum verification. **CVE ID : CVE-2023-23120**	https://www.trendnet.com/support/	H-TRE-TV-I-270223/2023
Vendor: ui					
Product: af-2x					
Affected Version(s): -					
Improper Validation of Integrity Check Value	02-Feb-2023	5.9	The use of the cyclic redundancy check (CRC) algorithm for integrity check during firmware update makes Ubiquiti airFiber AF2X Radio firmware version 3.2.2 and earlier vulnerable to firmware modification attacks. An attacker can conduct a man-in-the-middle	https://community.ui.com/tags/security/releases	H-UI-AF-2-270223/2024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(MITM) attack to modify the new firmware image and bypass the checksum verification. **CVE ID : CVE-2023-23119**		
Product: er-10x					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	H-UI-ER-1-270223/2025
Product: er-12					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-	H-UI-ER-1-270223/2026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	965a85633b5f	
Product: er-12p					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	H-UI-ER-1-270223/2027
Product: er-4					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-	H-UI-ER-4-270223/2028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	965a85633b5f	
Product: er-6p					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	H-UI-ER-6-270223/2029
Product: er-8-xg					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-	H-UI-ER-8-270223/2030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	4da4-9a21-965a85633b5f	
Product: er-x					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	H-UI-ER-X-270223/2031
Product: er-x-sfp					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e	H-UI-ER-X-270223/2032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	3b-718c-4da4-9a21-965a85633b5f	
Product: usg					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	H-UI-USG-270223/2033
Product: usg-pro-4					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their	https://community.ui.com/releases/Security-Advisory-Bulletin-028-	H-UI-USG--270223/2034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	028/696e4e3b-718c-4da4-9a21-965a85633b5f	
Operating System					
Vendor: ami					
Product: megarac_sp-x					
Affected Version(s): 12					
Insufficiently Protected Credentials	15-Feb-2023	7.5	AMI MegaRAC SPX devices allow Password Disclosure through Redfish. The fixed versions are SPx_12-update-7.00 and SPx_13-update-5.00. **CVE ID : CVE-2023-25191**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023002.pdf	O-AMI-MEGA-270223/2035
Exposure of Resource to Wrong Sphere	15-Feb-2023	5.3	AMI MegaRAC SPX devices allow User Enumeration through Redfish. The fixed versions are SPx12-update-7.00 and SPx13-update-5.00. **CVE ID : CVE-2023-25192**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023002.pdf	O-AMI-MEGA-270223/2036
Affected Version(s): 13					
Insufficiently Protected Credentials	15-Feb-2023	7.5	AMI MegaRAC SPX devices allow Password Disclosure through Redfish. The fixed	https://9443417.fs1.hubspotusercontent-	O-AMI-MEGA-270223/2037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions are SPx_12-update-7.00 and SPx_13-update-5.00. **CVE ID : CVE-2023-25191**	na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023002.pdf	
Exposure of Resource to Wrong Sphere	15-Feb-2023	5.3	AMI MegaRAC SPX devices allow User Enumeration through Redfish. The fixed versions are SPx12-update-7.00 and SPx13-update-5.00. **CVE ID : CVE-2023-25192**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023002.pdf	O-AMI-MEGA-270223/2038
Vendor: Apple					
Product: iphone_os					
Affected Version(s): -					
N/A	09-Feb-2023	9.8	External Control of Critical State Data, Improper Control of Generation of Code ('Code Injection') vulnerability in YugaByte, Inc. Yugabyte DB on Windows, Linux, MacOS, iOS (DevopsBase.Java:execCommand, TableManager.Java:runCommand modules) allows API Manipulation, Privilege Abuse. This vulnerability is associated with program files backup.Py. This issue affects Yugabyte DB: Lesser then 2.2.	N/A	O-APP-IPHO-270223/2039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0575		
Product: macos					
Affected Version(s): -					
N/A	09-Feb-2023	9.8	External Control of Critical State Data, Improper Control of Generation of Code ('Code Injection') vulnerability in YugaByte, Inc. Yugabyte DB on Windows, Linux, MacOS, iOS (DevopsBase.Java:execCommand, TableManager.Java:runCommand modules) allows API Manipulation, Privilege Abuse. This vulnerability is associated with program files backup.Py. This issue affects Yugabyte DB: Lesser then 2.2. **CVE ID : CVE-2023-0575**	N/A	O-APP-MACO-270223/2040
Vendor: arraynetworks					
Product: arrayos_ag					
Affected Version(s): * Up to (including) 9.4.0.470					
Out-of-bounds Write	03-Feb-2023	4.9	The user interface of Array Networks AG Series and vxAG through 9.4.0.470 could allow a remote attacker to use the gdb tool to overwrite the backend function call stack after accessing the system with administrator	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Net	O-ARR-ARRA-270223/2041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges. A successful exploit could leverage this vulnerability in the backend binary file that handles the user interface to a cause denial of service attack. This is fixed in AG 9.4.0.481. **CVE ID : CVE-2023-24613**	works_Security_Advisory_for_UI_Stack_Overflow_Vulnerability_ID-128285_V1.0.pdf	
Vendor: baicells					
Product: neutrino_430_firmware					
Affected Version(s): * Up to (including) qrtb_2.12.7					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Feb-2023	10	Baicells Nova 436Q, Nova 430E, Nova 430I, and Neutrino 430 LTE TDD eNodeB devices with firmware through QRTB 2.12.7 are vulnerable to remote shell code exploitation via HTTP command injections. Commands are executed using pre-login execution and executed with root permissions. The following methods below have been tested and validated by a 3rd party analyst and has been confirmed exploitable special thanks to Rustam Amin for providing the steps to reproduce. **CVE ID : CVE-2023-0776**	https://baicells.com/Service/Firmware	O-BAI-NEUT-270223/2042
Product: nova430e_firmware					
Affected Version(s): * Up to (including) qrtb_2.12.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Feb-2023	10	Baicells Nova 436Q, Nova 430E, Nova 430I, and Neutrino 430 LTE TDD eNodeB devices with firmware through QRTB 2.12.7 are vulnerable to remote shell code exploitation via HTTP command injections. Commands are executed using pre-login execution and executed with root permissions. The following methods below have been tested and validated by a 3rd party analyst and has been confirmed exploitable special thanks to Rustam Amin for providing the steps to reproduce. **CVE ID : CVE-2023-0776**	https://baicells.com/Service/Firmware	O-BAI-NOVA-270223/2043
Product: nova430l_firmware					
Affected Version(s): * Up to (including) qrtb_2.12.7					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Feb-2023	10	Baicells Nova 436Q, Nova 430E, Nova 430I, and Neutrino 430 LTE TDD eNodeB devices with firmware through QRTB 2.12.7 are vulnerable to remote shell code exploitation via HTTP command injections. Commands are executed using pre-login execution and executed with root permissions. The following methods below have been tested	https://baicells.com/Service/Firmware	O-BAI-NOVA-270223/2044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and validated by a 3rd party analyst and has been confirmed exploitable special thanks to Rustam Amin for providing the steps to reproduce. **CVE ID : CVE-2023-0776**		
Product: nova436q_firmware					
Affected Version(s): * Up to (including) qrtb_2.12.7					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Feb-2023	10	Baicells Nova 436Q, Nova 430E, Nova 430I, and Neutrino 430 LTE TDD eNodeB devices with firmware through QRTB 2.12.7 are vulnerable to remote shell code exploitation via HTTP command injections. Commands are executed using pre-login execution and executed with root permissions. The following methods below have been tested and validated by a 3rd party analyst and has been confirmed exploitable special thanks to Rustam Amin for providing the steps to reproduce. **CVE ID : CVE-2023-0776**	https://baicells.com/Service/Firmware	O-BAI-NOVA-270223/2045
Vendor: bdcom					
Product: 1704-wgl_firmware					
Affected Version(s): 2.0.6314					
N/A	03-Feb-2023	7.5	A vulnerability was found in BDCOM 1704-	N/A	O-BDC-1704-270223/2046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WGL 2.0.6314. It has been classified as critical. This affects an unknown part of the file /param.file.tgz of the component Backup File Handler. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The identifier VDB-220101 was assigned to this vulnerability. **CVE ID : CVE-2023-0659**		
Vendor: bosswerk					
Product: inverter_firmware					
Affected Version(s): mw3_15u_5406_1.47					
Use of Hard-coded Credentials	13-Feb-2023	6.8	A vulnerability was found in Deye/Revolt/Bosswerk Inverter MW3_15U_5406_1.47/ MW3_15U_5406_1.471. It has been rated as problematic. This issue affects some unknown processing of the component Access Point Setting Handler. The manipulation with the input 12345678 leads to use of hard-coded password. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. Upgrading to version MW3_16U_5406_1.53 is	N/A	O-BOS-INVE-270223/2047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-220769 was assigned to this vulnerability. **CVE ID : CVE-2023-0808**		
Affected Version(s): mw3_15u_5406_1.471					
Use of Hard-coded Credentials	13-Feb-2023	6.8	A vulnerability was found in Deye/Revolt/Bosswerk Inverter MW3_15U_5406_1.47/ MW3_15U_5406_1.471. It has been rated as problematic. This issue affects some unknown processing of the component Access Point Setting Handler. The manipulation with the input 12345678 leads to use of hard-coded password. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. Upgrading to version MW3_16U_5406_1.53 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-220769 was assigned to this vulnerability.	N/A	O-BOS-INVE-270223/2048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0808		
Vendor: Cisco					
Product: 807_industrial_integrated_services_router_firmware					
Affected Version(s): * Up to (excluding) 15.9\\(3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-807_-270223/2049
Affected Version(s): 15.9\\(3\\)m					
Improper Neutralization of Special	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an	https://sec.cloudapps.cisco.com/security/center/	O-CIS-807_-270223/2050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	
Affected Version(s): 15.9\\(3\\)m1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-807_-270223/2051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Affected Version(s): 15.9\\(3\\)m2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-807_-270223/2052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Affected Version(s): 15.9\\(3\\)m2a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-807_-270223/2053
Affected Version(s): 15.9\\(3\\)m3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-807_-270223/2054
Affected Version(s): 15.9\\(3\\)m4					
Improper Neutralization of Special Elements used in an OS Command ('OS	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-807_-270223/2055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Affected Version(s): 15.9\\(3\\)m4a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-807_-270223/2056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Affected Version(s): 15.9\\(3\\)m5					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-807_-270223/2057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20076		
Affected Version(s): 15.9\\(3\\)m6a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-807_-270223/2058
Affected Version(s): 15.9\\(3\\)m6b					
Improper Neutralization of Special Elements used in an	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-807_-270223/2059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	visory/cisco-sa-iox-8whGn5dL	
Product: 809_industrial_integrated_services_router_firmware					
Affected Version(s): * Up to (excluding) 15.9\\(3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-809_-270223/2060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Affected Version(s): 15.9\\(3\\)m					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-809_-270223/2061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Affected Version(s): 15.9\\(3\\)m1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-809_-270223/2062
Affected Version(s): 15.9\\(3\\)m2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-809_-270223/2063
Affected Version(s): 15.9\\(3\\)m2a					
Improper Neutralization of Special Elements used in an OS Command ('OS	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-809_-270223/2064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Affected Version(s): 15.9\\(3\\)m3					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-809_-270223/2065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Affected Version(s): 15.9\\(3\\)m4					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-809_-270223/2066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20076		
Affected Version(s): 15.9\\(3\\)m4a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-809_-270223/2067
Affected Version(s): 15.9\\(3\\)m5					
Improper Neutralization of Special Elements used in an	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-809_-270223/2068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	visory/cisco-sa-iox-8whGn5dL	
Affected Version(s): 15.9\\(3\\)m6a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-809_-270223/2069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Affected Version(s): 15.9\\(3\\)m6b					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-809_-270223/2070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Product: 829_industrial_integrated_services_router_firmware					
Affected Version(s): * Up to (excluding) 15.9\\(3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-829_-270223/2071
Affected Version(s): 15.9\\(3\\)m					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-829_-270223/2072
Affected Version(s): 15.9\\(3\\)m1					
Improper Neutralization of Special Elements used in an OS Command ('OS	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-829_-270223/2073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Affected Version(s): 15.9\\(3\\)m2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-829_-270223/2074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Affected Version(s): 15.9\\(3\\)m2a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-829_-270223/2075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20076		
Affected Version(s): 15.9\\(3\\)m3					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-829_-270223/2076
Affected Version(s): 15.9\\(3\\)m4					
Improper Neutralization of Special Elements used in an	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-829_-270223/2077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	visory/cisco-sa-iox-8whGn5dL	
Affected Version(s): 15.9\\(3\\)m4a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-829_-270223/2078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Affected Version(s): 15.9\\(3\\)m5					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-829_-270223/2079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Affected Version(s): 15.9\\(3\\)m6a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-829_-270223/2080
Affected Version(s): 15.9\\(3\\)m6b					
Improper Neutralizat	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application	https://sec.cloudapps.cis	O-CIS-829_-270223/2081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	co.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	
Product: cgr1000_firmware					
Affected Version(s): * Up to (excluding) 1.16.0.1					
Improper Neutralization of Special Elements used in an OS Command ('OS	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-CGR1-270223/2082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Product: cgr1240_firmware					
Affected Version(s): * Up to (excluding) 1.16.0.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-CGR1-270223/2083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Product: ios_xe					
Affected Version(s): * Up to (excluding) 17.6.5					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-IOS_-270223/2084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying host operating system. **CVE ID : CVE-2023-20076**		
Affected Version(s): 17.10.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-IOS_-270223/2085
Affected Version(s): From (including) 17.9.0 Up to (excluding) 17.9.2					
Improper Neutralization of Special	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an	https://sec.cloudapps.cisco.com/security/center/	O-CIS-IOS_-270223/2086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**	content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	
Product: ir510_wpan_firmware					
Affected Version(s): * Up to (excluding) 1.10.0.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-2023	8.8	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL	O-CIS-IR51-270223/2087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system. **CVE ID : CVE-2023-20076**		
Vendor: contec					
Product: solarview_compact_firmware					
Affected Version(s): * Up to (including) 6.00					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Feb-2023	9.8	There is a command injection vulnerability in SolarView Compact through 6.00, attackers can execute commands by bypassing internal restrictions through downloader.php. **CVE ID : CVE-2023-23333**	N/A	O-CON-SOLA-270223/2088
Vendor: controlbyweb					
Product: x-400_firmware					
Affected Version(s): * Up to (excluding) 2.8					
Improper Neutralization of Input During Web Page	13-Feb-2023	6.1	Control By Web X-400 devices are vulnerable to a cross-site scripting attack, which could result in private and session information	N/A	O-CON-X-40-270223/2089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			being transferred to the attacker. **CVE ID : CVE-2023-23553**		
Product: x-600m_firmware					
Affected Version(s): * Up to (excluding) 1.16.00					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Control By Web X-600M devices run Lua scripts and are vulnerable to code injection, which could allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2023-23551**	N/A	O-CON-X-60-270223/2090
Vendor: D-link					
Product: dwl-2600ap_firmware					
Affected Version(s): 4.2.0.17					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Feb-2023	7.8	A command injection vulnerability in the firmware_update command, in the device's restricted telnet interface, allows an authenticated attacker to execute arbitrary commands as root. **CVE ID : CVE-2023-0127**	N/A	O-D-L-DWL--270223/2091
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
N/A	14-Feb-2023	9.1	HAProxy before 2.7.3 may allow a bypass of access control because HTTP/1 headers are inadvertently lost in some situations, aka	https://git.haproxy.org/?p=haproxy-2.7.git;a=commit;h=a0e561ad7f29e	O-DEB-DEBI-270223/2092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"request smuggling." The HTTP header parsers in HAProxy may accept empty header field names, which could be used to truncate the list of HTTP headers and thus make some headers disappear after being parsed and processed for HTTP/1.0 and HTTP/1.1. For HTTP/2 and HTTP/3, the impact is limited because the headers disappear before being parsed and processed, as if they had not been sent by the client. The fixed versions are 2.7.3, 2.6.9, 2.5.12, 2.4.22, 2.2.29, and 2.0.31. **CVE ID : CVE-2023-25725**	d50c473f5a9da664267b60d1112	
Observable Discrepancy	15-Feb-2023	7.5	A timing side-channel in the handling of RSA ClientKeyExchange messages was discovered in GnuTLS. This side-channel can be sufficient to recover the key encrypted in the RSA ciphertext across a network in a Bleichenbacher style attack. To achieve a successful decryption the attacker would need to send a large amount of specially crafted messages to the vulnerable server. By	https://gitlab.com/gnutls/gnutls/-/issues/1050, https://github.com/tlsfuzzer/tlsfuzzer/pull/679	O-DEB-DEBI-270223/2093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recovering the secret from the ClientKeyExchange message, the attacker would be able to decrypt the application data exchanged over that connection. **CVE ID : CVE-2023-0361**		
Allocation of Resources Without Limits or Throttling	01-Feb-2023	7.5	In Django 3.2 before 3.2.17, 4.0 before 4.0.9, and 4.1 before 4.1.6, the parsed values of Accept-Language headers are cached in order to avoid repetitive parsing. This leads to a potential denial-of-service vector via excessive memory usage if the raw value of Accept-Language headers is very large. **CVE ID : CVE-2023-23969**	https://docs.djangoproject.com/en/4.1/releases/security/, https://www.djangoproject.com/weblog/2023/feb/01/security-releases/	O-DEB-DEBI-270223/2094
Uncontrolled Resource Consumption	15-Feb-2023	7.5	An issue was discovered in the Multipart Request Parser in Django 3.2 before 3.2.18, 4.0 before 4.0.10, and 4.1 before 4.1.7. Passing certain inputs (e.g., an excessive number of parts) to multipart forms could result in too many open files or memory exhaustion, and provided a potential vector for a denial-of-service attack.	https://docs.djangoproject.com/en/4.1/releases/security/, https://www.djangoproject.com/weblog/2023/feb/14/security-releases/	O-DEB-DEBI-270223/2095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24580		
Affected Version(s): 11.0					
N/A	14-Feb-2023	9.1	HAProxy before 2.7.3 may allow a bypass of access control because HTTP/1 headers are inadvertently lost in some situations, aka "request smuggling." The HTTP header parsers in HAProxy may accept empty header field names, which could be used to truncate the list of HTTP headers and thus make some headers disappear after being parsed and processed for HTTP/1.0 and HTTP/1.1. For HTTP/2 and HTTP/3, the impact is limited because the headers disappear before being parsed and processed, as if they had not been sent by the client. The fixed versions are 2.7.3, 2.6.9, 2.5.12, 2.4.22, 2.2.29, and 2.0.31. **CVE ID : CVE-2023-25725**	https://git.haproxy.org/?p=haproxy-2.7.git;a=commit;h=a0e561ad7f29ed50c473f5a9da664267b60d1112	O-DEB-DEBI-270223/2096
Vendor: Dell					
Product: emc_data_domain_os					
Affected Version(s): * Up to (excluding) 6.2.1.90					
Improper Neutralization of Special Elements	01-Feb-2023	8.8	Dell EMC prior to version DDOS 7.9 contain(s) an OS command injection Vulnerability. An	https://www.dell.com/support/kbdoc/en-us/0002012	O-DEL-EMC_-270223/2097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			authenticated non admin attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. **CVE ID : CVE-2023-23692**	96/dsa-2022-187-dell-technologies-powerprotect-data-domain-security-update-for-multiple-third-party-component-vulnerabilities	
Affected Version(s): From (including) 7.0.0.0 Up to (excluding) 7.9.0.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Feb-2023	8.8	Dell EMC prior to version DDOS 7.9 contain(s) an OS command injection Vulnerability. An authenticated non admin attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. **CVE ID : CVE-2023-23692**	https://www.dell.com/support/kbdoc/en-us/000201296/dsa-2022-187-dell-technologies-powerprotect-data-domain-security-update-for-multiple-third-party-component-vulnerabilities	O-DEL-EMC_-270223/2098
Affected Version(s): From (including) 7.7.1 Up to (excluding) 7.7.3					
Improper Neutralization of Special Elements used in an	01-Feb-2023	8.8	Dell EMC prior to version DDOS 7.9 contain(s) an OS command injection Vulnerability. An authenticated non	https://www.dell.com/support/kbdoc/en-us/000201296/dsa-	O-DEL-EMC_-270223/2099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			admin attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. **CVE ID : CVE-2023-23692**	2022-187-dell-technologies-powerprotect-data-domain-security-update-for-multiple-third-party-component-vulnerabilities	
Product: emc_powerscale_onefs					
Affected Version(s): From (including) 9.1.0.0 Up to (excluding) 9.1.0.27					
Insertion of Sensitive Information into Log File	01-Feb-2023	8.8	Dell PowerScale OneFS 9.0.0.x - 9.4.0.x contain an insertion of sensitive information into log file vulnerability in celog. A low privileges user could potentially exploit this vulnerability, leading to information disclosure and escalation of privileges. **CVE ID : CVE-2023-22575**	https://www.dell.com/support/kbdoc/en-us/000207863/dell-powerscale-onefs-security-updates-for-multiple-security	O-DEL-EMC_-270223/2100
Insertion of Sensitive Information into Log File	01-Feb-2023	8.1	Dell PowerScale OneFS 9.0.0.x - 9.4.0.x contain an insertion of sensitive information into log file vulnerability in platform API of IPMI module. A low-privileged user with permission to read logs on the cluster could potentially exploit this vulnerability, leading to	https://www.dell.com/support/kbdoc/en-us/000207863/dell-powerscale-onefs-security-updates-for-multiple-security	O-DEL-EMC_-270223/2101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Information disclosure and denial of service. **CVE ID : CVE-2023-22574**		
Insertion of Sensitive Information into Log File	01-Feb-2023	7.8	Dell PowerScale OneFS 9.1.0.x-9.4.0.x contain an insertion of sensitive information into log file vulnerability in change password api. A low privilege local attacker could potentially exploit this vulnerability, leading to system takeover. **CVE ID : CVE-2023-22572**	https://www.dell.com/support/kbdoc/en-us/000207863/dell-powerscale-onefs-security-updates-for-multiple-security	O-DEL-EMC_-270223/2102
Insertion of Sensitive Information into Log File	01-Feb-2023	5.5	Dell PowerScale OneFS 9.0.0.x-9.4.0.x contain an insertion of sensitive information into log file vulnerability in cloudpool. A low privileged local attacker could potentially exploit this vulnerability, leading to sensitive information disclosure. **CVE ID : CVE-2023-22573**	https://www.dell.com/support/kbdoc/en-us/000207863/dell-powerscale-onefs-security-updates-for-multiple-security	O-DEL-EMC_-270223/2103
Affected Version(s): From (including) 9.2.1.0 Up to (excluding) 9.2.1.20					
Insertion of Sensitive Information into Log File	01-Feb-2023	8.8	Dell PowerScale OneFS 9.0.0.x - 9.4.0.x contain an insertion of sensitive information into log file vulnerability in celog. A low privileges user could potentially exploit this vulnerability, leading to information disclosure	https://www.dell.com/support/kbdoc/en-us/000207863/dell-powerscale-onefs-security-updates-for-	O-DEL-EMC_-270223/2104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and escalation of privileges. **CVE ID : CVE-2023-22575**	multiple-security	
Insertion of Sensitive Information into Log File	01-Feb-2023	8.1	Dell PowerScale OneFS 9.0.0.x - 9.4.0.x contain an insertion of sensitive information into log file vulnerability in platform API of IPMI module. A low-privileged user with permission to read logs on the cluster could potentially exploit this vulnerability, leading to Information disclosure and denial of service. **CVE ID : CVE-2023-22574**	https://www.dell.com/support/kbdoc/en-us/000207863/dell-powerscale-onefs-security-updates-for-multiple-security	O-DEL-EMC_-270223/2105
Insertion of Sensitive Information into Log File	01-Feb-2023	7.8	Dell PowerScale OneFS 9.1.0.x-9.4.0.x contain an insertion of sensitive information into log file vulnerability in change password api. A low privilege local attacker could potentially exploit this vulnerability, leading to system takeover. **CVE ID : CVE-2023-22572**	https://www.dell.com/support/kbdoc/en-us/000207863/dell-powerscale-onefs-security-updates-for-multiple-security	O-DEL-EMC_-270223/2106
Insertion of Sensitive Information into Log File	01-Feb-2023	5.5	Dell PowerScale OneFS 9.0.0.x-9.4.0.x contain an insertion of sensitive information into log file vulnerability in cloudpool. A low privileged local attacker could potentially exploit this	https://www.dell.com/support/kbdoc/en-us/000207863/dell-powerscale-onefs-security-	O-DEL-EMC_-270223/2107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, leading to sensitive information disclosure. **CVE ID : CVE-2023-22573**	updates-for-multiple-security	
Affected Version(s): From (including) 9.4.0.0 Up to (excluding) 9.4.0.11					
Insertion of Sensitive Information into Log File	01-Feb-2023	8.8	Dell PowerScale OneFS 9.0.0.x - 9.4.0.x contain an insertion of sensitive information into log file vulnerability in celog. A low privileges user could potentially exploit this vulnerability, leading to information disclosure and escalation of privileges. **CVE ID : CVE-2023-22575**	https://www.dell.com/support/kbdoc/en-us/000207863/dell-powerscale-onefs-security-updates-for-multiple-security	O-DEL-EMC_-270223/2108
Insertion of Sensitive Information into Log File	01-Feb-2023	8.1	Dell PowerScale OneFS 9.0.0.x - 9.4.0.x contain an insertion of sensitive information into log file vulnerability in platform API of IPMI module. A low-privileged user with permission to read logs on the cluster could potentially exploit this vulnerability, leading to Information disclosure and denial of service. **CVE ID : CVE-2023-22574**	https://www.dell.com/support/kbdoc/en-us/000207863/dell-powerscale-onefs-security-updates-for-multiple-security	O-DEL-EMC_-270223/2109
Insertion of Sensitive Information into Log File	01-Feb-2023	7.8	Dell PowerScale OneFS 9.1.0.x-9.4.0.x contain an insertion of sensitive information into log file vulnerability in change password api. A low	https://www.dell.com/support/kbdoc/en-us/000207863/dell-	O-DEL-EMC_-270223/2110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege local attacker could potentially exploit this vulnerability, leading to system takeover. **CVE ID : CVE-2023-22572**	powerscale-onefs-security-updates-for-multiple-security	
Insertion of Sensitive Information into Log File	01-Feb-2023	5.5	Dell PowerScale OneFS 9.0.0.x-9.4.0.x contain an insertion of sensitive information into log file vulnerability in cloudpool. A low privileged local attacker could potentially exploit this vulnerability, leading to sensitive information disclosure. **CVE ID : CVE-2023-22573**	https://www.dell.com/support/kbdoc/en-us/000207863/dell-powerscale-onefs-security-updates-for-multiple-security	O-DEL-EMC_-270223/2111
Product: enterprise_sonic_distribution					
Affected Version(s): From (including) 3.5.3 Up to (excluding) 4.0.3					
Uncontrolled Resource Consumption	02-Feb-2023	7.5	Dell Enterprise SONiC OS, 3.5.3, 4.0.0, 4.0.1, 4.0.2, contains an "Uncontrolled Resource Consumption vulnerability" in authentication component. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to uncontrolled resource consumption by creating permanent home directories for unauthenticated users.	https://www.dell.com/support/kbdoc/en-us/000208165/dsa-2023-039-dell-emc-enterprise-sonic-security-update-for-an-uncontrolled-resource-consumption-vulnerability	O-DEL-ENTE-270223/2112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24574		
Vendor: deyeinverter					
Product: inverter_firmware					
Affected Version(s): mw3_15u_5406_1.47					
Use of Hard-coded Credentials	13-Feb-2023	6.8	A vulnerability was found in Deye/Revolt/Bosswerk Inverter MW3_15U_5406_1.47/ MW3_15U_5406_1.471. It has been rated as problematic. This issue affects some unknown processing of the component Access Point Setting Handler. The manipulation with the input 12345678 leads to use of hard-coded password. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. Upgrading to version MW3_16U_5406_1.53 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-220769 was assigned to this vulnerability. **CVE ID : CVE-2023-0808**	N/A	O-DEY-INVE-270223/2113
Affected Version(s): mw3_15u_5406_1.471					
Use of Hard-	13-Feb-2023	6.8	A vulnerability was found in Deye/Revolt/Bosswerk	N/A	O-DEY-INVE-270223/2114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			Inverter MW3_15U_5406_1.47/ MW3_15U_5406_1.471. It has been rated as problematic. This issue affects some unknown processing of the component Access Point Setting Handler. The manipulation with the input 12345678 leads to use of hard-coded password. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. Upgrading to version MW3_16U_5406_1.53 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-220769 was assigned to this vulnerability. **CVE ID : CVE-2023-0808**		
Vendor: Dlink					
Product: dir-605l_firmware					
Affected Version(s): 2.13b01					
Out-of-bounds Write	10-Feb-2023	9.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the curTime parameter at /goform/formSetACLFilter.	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--270223/2115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24348		
Out-of-bounds Write	10-Feb-2023	9.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the curTime parameter at /goform/formSetRoute. **CVE ID : CVE-2023-24349**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--270223/2116
Out-of-bounds Write	10-Feb-2023	9.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the config.smtp_email_subject parameter at /goform/formSetEmail. **CVE ID : CVE-2023-24350**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--270223/2117
Out-of-bounds Write	10-Feb-2023	9.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the FILECODE parameter at /goform/formLogin. **CVE ID : CVE-2023-24351**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--270223/2118
Out-of-bounds Write	10-Feb-2023	9.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the webpage parameter at /goform/formWPS. **CVE ID : CVE-2023-24352**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--270223/2119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-Feb-2023	8.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the curTime parameter at /goform/formSchedule. **CVE ID : CVE-2023-24343**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--270223/2120
Out-of-bounds Write	10-Feb-2023	8.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the webpage parameter at /goform/formWlanGuestSetup. **CVE ID : CVE-2023-24344**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--270223/2121
Out-of-bounds Write	10-Feb-2023	8.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the curTime parameter at /goform/formSetWanDhcpplus. **CVE ID : CVE-2023-24345**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--270223/2122
Out-of-bounds Write	10-Feb-2023	8.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the wan_connected parameter at /goform/formEasySetupWizard3. **CVE ID : CVE-2023-24346**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--270223/2123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-Feb-2023	8.8	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the webpage parameter at /goform/formSetWanDhcpplus. **CVE ID : CVE-2023-24347**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--270223/2124
Vendor: F5					
Product: big-ip_10000s_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2125
Product: big-ip_10200v-ssl_firmware					
Affected Version(s): -					
NULL Pointer	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2,	https://my.f5.com/mana	O-F5-BIG--270223/2126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	ge/s/article /K37708118	
Product: big-ip_10200v_firmware					
Affected Version(s): -					
NULL Pointer Dereferenc e	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached	https://my.f 5.com/mana ge/s/article /K37708118	O-F5-BIG-- 270223/2127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: big-ip_12000_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2128
Product: big-ip_5000s_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: big-ip_5200v-ssl_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: big-ip_5200v_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2131
Product: big-ip_7000s_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: big-ip_7200v-ssl_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2133
Product: big-ip_7200v_firmware					
Affected Version(s): -					
NULL Pointer	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3,	https://my.f5.com/mana	O-F5-BIG--270223/2134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	ge/s/article /K37708118	
Product: big-ip_i10600_firmware					
Affected Version(s): -					
NULL Pointer Dereferenc e	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f 5.com/mana ge/s/article /K37708118	O-F5-BIG-- 270223/2135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: big-ip_i10800_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2136
Product: big-ip_i11600_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: big-ip_i11800_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2138
Product: big-ip_i15600_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2139
Product: big-ip_i15800_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: big-ip_i5600_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2141
Product: big-ip_i5800_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1,	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: big-ip_i7600_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: big-ip_i7800_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	O-F5-BIG--270223/2144
Product: f5os-a					
Affected Version(s): From (including) 1.2.0 Up to (excluding) 1.3.0					
Improper Neutralization of Special Elements used in a Command ('Comman	01-Feb-2023	7.8	On F5OS-A beginning in version 1.2.0 to before 1.3.0 and F5OS-C beginning in version 1.3.0 to before 1.5.0, processing F5OS tenant file names may allow for command injection. Note: Software versions	https://my.f5.com/manage/s/article/K06345931	O-F5-F5OS-270223/2145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22657**		
Product: f5os-c					
Affected Version(s): From (including) 1.3.0 Up to (excluding) 1.5.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Feb-2023	7.8	On F5OS-A beginning in version 1.2.0 to before 1.3.0 and F5OS-C beginning in version 1.3.0 to before 1.5.0, processing F5OS tenant file names may allow for command injection. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22657**	https://my.f5.com/manage/s/article/K06345931	O-F5-F5OS-270223/2146
Product: r10600_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to	https://my.f5.com/manage/s/article/K37708118	O-F5-R106-270223/2147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: r10800_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	O-F5-R108-270223/2148
Product: r10900_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3,	https://my.f5.com/manage/s/article/K37708118	O-F5-R109-270223/2149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: r5600_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K37708118	O-F5-R560-270223/2150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: r5800_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	O-F5-R580-270223/2151
Product: r5900_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting	https://my.f5.com/manage/s/article/K37708118	O-F5-R590-270223/2152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: velos_bx110_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	O-F5-VELO-270223/2153
Product: viprion_b2100_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	O-F5-VIPR-270223/2154
Product: viprion_b2150_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management	https://my.f5.com/manage/s/article/K37708118	O-F5-VIPR-270223/2155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: viprion_b2250_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**	https://my.f5.com/manage/s/article/K37708118	O-F5-VIPR-270223/2156
Product: viprion_b4300_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1,	https://my.f5.com/manage/s/article/K37708118	O-F5-VIPR-270223/2157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Product: viprion_b4450_firmware					
Affected Version(s): -					
NULL Pointer Dereference	01-Feb-2023	7.5	On BIG-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all version of 13.1.x, when a DNS profile with the Rapid Response Mode setting enabled is configured on a virtual server with hardware SYN cookies enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K37708118	O-F5-VIPR-270223/2158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22839**		
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 36					
Allocation of Resources Without Limits or Throttling	04-Feb-2023	7.5	hb-ot-layout-gsubgpos.hh in HarfBuzz through 6.0.0 allows attackers to trigger O(n^2) growth via consecutive marks during the process of looking back for base glyphs when attaching marks. **CVE ID : CVE-2023-25193**	https://github.com/harfbuzz/harfbuzz/commit/85be877925ddbf34f74a1229f3ca1716bb6170dc, https://chromium.googlesource.com/chromium/src/+/e1f324aa681af54101c1f2d173d92adb80e37088/DEPS#361	O-FED-FEDO-270223/2159
Vendor: Freebsd					
Product: freebsd					
Affected Version(s): 12.3					
N/A	08-Feb-2023	6.5	When GELI reads a key file from standard input, it does not reuse the key file to initialize multiple providers at once resulting in the second and subsequent devices silently using a NULL key as the user key file. If a user only uses a key file without a user passphrase, the master key is encrypted	https://security.FreeBSD.org/advisories/FreeBSD-SA-23:01.geli.asc	O-FRE-FREE-270223/2160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with an empty key file allowing trivial recovery of the master key. **CVE ID : CVE-2023-0751**		
Affected Version(s): 12.4					
N/A	08-Feb-2023	6.5	When GELI reads a key file from standard input, it does not reuse the key file to initialize multiple providers at once resulting in the second and subsequent devices silently using a NULL key as the user key file. If a user only uses a key file without a user passphrase, the master key is encrypted with an empty key file allowing trivial recovery of the master key. **CVE ID : CVE-2023-0751**	https://security.FreeBSD.org/advisories/FreeBSD-SA-23:01.geli.asc	O-FRE-FREE-270223/2161
Affected Version(s): 13.1					
N/A	08-Feb-2023	6.5	When GELI reads a key file from standard input, it does not reuse the key file to initialize multiple providers at once resulting in the second and subsequent devices silently using a NULL key as the user key file. If a user only uses a key file without a user passphrase, the master key is encrypted with an empty key file allowing trivial	https://security.FreeBSD.org/advisories/FreeBSD-SA-23:01.geli.asc	O-FRE-FREE-270223/2162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recovery of the master key. **CVE ID : CVE-2023-0751**		
Vendor: Google					
Product: android					
Affected Version(s): -					
N/A	14-Feb-2023	8.3	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23374**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23374	O-GOO-ANDR-270223/2163
N/A	07-Feb-2023	6.5	Inappropriate implementation in Full screen mode in Google Chrome on Android prior to 110.0.5481.77 allowed a remote attacker to spoof the contents of the security UI via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-0697**	https://chromereleases.googleblog.com/2023/02/stable-channel-update-for-desktop.html, https://crbug.com/1341541	O-GOO-ANDR-270223/2164
Out-of-bounds Write	15-Feb-2023	5.5	In s2mpg11_pmic_probe of s2mpg11-regulator.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/pixel/2023-02-01	O-GOO-ANDR-270223/2165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android kernelAndroid ID: A-259323133References: N/A **CVE ID : CVE-2023-20949**		
Affected Version(s): 10.0					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2166
Affected Version(s): 11.0					
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2168
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2169
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**		
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2171
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2172
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**		
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2174
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2175
Improper Synchronization	06-Feb-2023	6.4	In ccu, there is a possible memory corruption due to a race condition. This could lead to local escalation	https://corp.mediatek.com/product-security-	O-GOO-ANDR-270223/2176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07512839; Issue ID: ALPS07512839. **CVE ID : CVE-2023-20607**	bulletin/February-2023	
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2177
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2178
Improper Restriction of	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing	https://corp.mediatek.com/product-	O-GOO-ANDR-270223/2179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	security-bulletin/February-2023	
Out-of-bounds Read	06-Feb-2023	4.4	In ccu, there is a possible out of bounds read due to a logic error. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570864; Issue ID: ALPS07570864. **CVE ID : CVE-2023-20609**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2180
Affected Version(s): 12.0					
N/A	09-Feb-2023	7.5	An improper implementation logic in Secure Folder prior to SMR Jan-2023 Release 1 allows the Secure Folder container remain unlocked under certain condition. **CVE ID : CVE-2023-21419**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-GOO-ANDR-270223/2181
Integer Overflow or	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could	https://corp.mediatek.com/product-security-	O-GOO-ANDR-270223/2182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	bulletin/February-2023	
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2183
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2185
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2186
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Feb-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07560720. **CVE ID : CVE-2023-20616**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2188
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2189
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**		
Improper Synchronization	06-Feb-2023	6.4	In ccu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07512839; Issue ID: ALPS07512839. **CVE ID : CVE-2023-20607**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2191
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2192
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469. **CVE ID : CVE-2023-20610**		
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2194
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2195
Improper Input Validation	06-Feb-2023	4.4	In apusys, there is a possible out of bounds read due to a missing bounds check. This	https://corp.mediatek.com/product-security-	O-GOO-ANDR-270223/2196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571104; Issue ID: ALPS07571104. **CVE ID : CVE-2023-20606**	bulletin/February-2023	
Out-of-bounds Read	06-Feb-2023	4.4	In ccu, there is a possible out of bounds read due to a logic error. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570864; Issue ID: ALPS07570864. **CVE ID : CVE-2023-20609**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2197
Affected Version(s): 12.1					
Improper Input Validation	06-Feb-2023	4.4	In apusys, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571104; Issue ID: ALPS07571104. **CVE ID : CVE-2023-20606**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 13.0					
N/A	15-Feb-2023	7.8	In permissions of AndroidManifest.xml, there is a possible way to grant signature permissions due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-244216503 **CVE ID : CVE-2023-20927**	https://source.android.com/security/bulletin/aaos/2023-02-01	O-GOO-ANDR-270223/2199
Integer Overflow or Wraparound	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494107; Issue ID: ALPS07494107. **CVE ID : CVE-2023-20602**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2200
Out-of-bounds Write	06-Feb-2023	6.7	In ged, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494067; Issue ID: ALPS07494067. **CVE ID : CVE-2023-20604**		
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629571; Issue ID: ALPS07629571. **CVE ID : CVE-2023-20612**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2202
Improper Input Validation	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628614; Issue ID: ALPS07628614. **CVE ID : CVE-2023-20613**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2203
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	O-GOO-ANDR-270223/2204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628615; Issue ID: ALPS07628615. **CVE ID : CVE-2023-20614**	bulletin/February-2023	
Out-of-bounds Write	06-Feb-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629572; Issue ID: ALPS07629572. **CVE ID : CVE-2023-20615**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2205
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519184; Issue ID: ALPS07519184. **CVE ID : CVE-2023-20618**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Locking	06-Feb-2023	6.7	In vcu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519159; Issue ID: ALPS07519159. **CVE ID : CVE-2023-20619**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2207
Use After Free	06-Feb-2023	6.4	In display drm, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363599; Issue ID: ALPS07363599. **CVE ID : CVE-2023-20608**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2208
Improper Synchronization	06-Feb-2023	6.4	In display drm, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363469; Issue ID: ALPS07363469.	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20610		
Improper Synchronization	06-Feb-2023	6.4	In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678. **CVE ID : CVE-2023-20611**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2210
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Feb-2023	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550104. **CVE ID : CVE-2023-20605**	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2211
Out-of-bounds Read	06-Feb-2023	4.4	In ccu, there is a possible out of bounds read due to a logic error. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/February-2023	O-GOO-ANDR-270223/2212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07570864; Issue ID: ALPS07570864. **CVE ID : CVE-2023-20609**		
Vendor: HP					
Product: hp-ux					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	03-Feb-2023	9.8	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system with a specially crafted sequence of serialized objects. IBM X-Force ID: 245513. **CVE ID : CVE-2023-23477**	https://www.ibm.com/support/pages/node/6891111, https://exchange.xforce.ibmcloud.com/vulnerabilities/245513	O-HP-HP-U-270223/2213
Vendor: IBM					
Product: aix					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	03-Feb-2023	9.8	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system with a specially crafted sequence of serialized objects. IBM X-Force ID: 245513. **CVE ID : CVE-2023-23477**	https://www.ibm.com/support/pages/node/6891111, https://exchange.xforce.ibmcloud.com/vulnerabilities/245513	O-IBM-AIX-270223/2214
Improper Neutralization of Input During Web Page	08-Feb-2023	4.6	IBM Infosphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed	https://www.ibm.com/support/pages/node/6890711	O-IBM-AIX-270223/2215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 245423. **CVE ID : CVE-2023-23475**		
Product: i					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	03-Feb-2023	9.8	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system with a specially crafted sequence of serialized objects. IBM X-Force ID: 245513. **CVE ID : CVE-2023-23477**	https://www.ibm.com/support/pages/node/6891111, https://exchange.xforce.ibmcloud.com/vulnerabilities/245513	O-IBM-I-270223/2216
Product: z\/os					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	03-Feb-2023	9.8	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system with a specially crafted sequence of serialized objects. IBM X-Force ID: 245513. **CVE ID : CVE-2023-23477**	https://www.ibm.com/support/pages/node/6891111, https://exchange.xforce.ibmcloud.com/vulnerabilities/245513	O-IBM-Z\/O-270223/2217
Vendor: Linux					
Product: linux_kernel					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	09-Feb-2023	9.8	External Control of Critical State Data, Improper Control of Generation of Code ('Code Injection') vulnerability in YugaByte, Inc. Yugabyte DB on Windows, Linux, MacOS, iOS (DevopsBase.Java:execCommand, TableManager.Java:runCommand modules) allows API Manipulation, Privilege Abuse. This vulnerability is associated with program files backup.Py. This issue affects Yugabyte DB: Lesser then 2.2. **CVE ID : CVE-2023-0575**	N/A	O-LIN-LINU-270223/2218
Improper Control of Generation of Code ('Code Injection')	03-Feb-2023	9.8	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system with a specially crafted sequence of serialized objects. IBM X-Force ID: 245513. **CVE ID : CVE-2023-23477**	https://www.ibm.com/support/pages/node/6891111, https://exchange.xforce.ibmcloud.com/vulnerabilities/245513	O-LIN-LINU-270223/2219
Improper Neutralization of Input During	08-Feb-2023	4.6	IBM Infosphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows	https://www.ibm.com/support/pages/node/6890711	O-LIN-LINU-270223/2220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 245423. **CVE ID : CVE-2023-23475**		
Affected Version(s): * Up to (excluding) 6.2					
Divide By Zero	06-Feb-2023	5.5	A memory leak flaw and potential divide by zero and Integer overflow was found in the Linux kernel V4L2 and vivid test code functionality. This issue occurs when a user triggers ioctls, such as VIDIOC_S_DV_TIMINGS ioctl. This could allow a local user to crash the system if vivid test code enabled. **CVE ID : CVE-2023-0615**	N/A	O-LIN-LINU-270223/2221
Affected Version(s): * Up to (including) 6.1.9					
Use After Free	02-Feb-2023	4.6	The Linux kernel through 6.1.9 has a Use-After-Free in bigben_remove in drivers/hid/hid-bigbenff.c via a crafted USB device because the LED controllers remain registered for too long. **CVE ID : CVE-2023-25012**	https://lore.kernel.org/all/20230125-hid-unregister-leds-v1-1-9a5192dcef16@diag.uniroma1.it/	O-LIN-LINU-270223/2222
Affected Version(s): 6.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Divide By Zero	06-Feb-2023	5.5	A memory leak flaw and potential divide by zero and Integer overflow was found in the Linux kernel V4L2 and vivid test code functionality. This issue occurs when a user triggers ioctls, such as VIDIOC_S_DV_TIMINGS ioctl. This could allow a local user to crash the system if vivid test code enabled. **CVE ID : CVE-2023-0615**	N/A	O-LIN-LINU-270223/2223
Vendor: ls-electric					
Product: xbc-dn32u_firmware					
Affected Version(s): 01.80					
Missing Authentication for Critical Function	15-Feb-2023	9.8	LS ELECTRIC XBC-DN32U with operating system version 01.80 is missing authentication to create users on the PLC. This could allow an attacker to create and use an account with elevated privileges and take control of the device. **CVE ID : CVE-2023-22804**	N/A	O-LS--XBC--270223/2224
N/A	15-Feb-2023	9.8	LS ELECTRIC XBC-DN32U with operating system version 01.80 does not properly control access to the PLC over its internal XGT protocol. An attacker could control and tamper with the PLC by sending the	N/A	O-LS--XBC--270223/2225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packets to the PLC over its XGT protocol. **CVE ID : CVE-2023-22807**		
Missing Authentication for Critical Function	15-Feb-2023	9.1	LS ELECTRIC XBC-DN32U with operating system version 01.80 is missing authentication for its deletion command. This could allow an attacker to delete arbitrary files. **CVE ID : CVE-2023-0102**	N/A	O-LS--XBC--270223/2226
Access of Memory Location After End of Buffer	15-Feb-2023	7.5	If an attacker were to access memory locations of LS ELECTRIC XBC-DN32U with operating system version 01.80 that are outside of the communication buffer, the device stops operating. This could allow an attacker to cause a denial-of-service condition. **CVE ID : CVE-2023-0103**	N/A	O-LS--XBC--270223/2227
Missing Authentication for Critical Function	15-Feb-2023	7.5	LS ELECTRIC XBC-DN32U with operating system version 01.80 is missing authentication to perform critical functions to the PLC. This could allow an attacker to change the PLC's mode arbitrarily. **CVE ID : CVE-2023-22803**	N/A	O-LS--XBC--270223/2228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	15-Feb-2023	7.5	LS ELECTRIC XBC-DN32U with operating system version 01.80 transmits sensitive information in cleartext when communicating over its XGT protocol. This could allow an attacker to gain sensitive information such as user credentials. **CVE ID : CVE-2023-22806**	N/A	O-LS--XBC--270223/2229
N/A	15-Feb-2023	4.3	LS ELECTRIC XBC-DN32U with operating system version 01.80 has improper access control to its read prohibition feature. This could allow a remote attacker to remotely set the feature to lock users out of reading data from the device. **CVE ID : CVE-2023-22805**	N/A	O-LS--XBC--270223/2230
Vendor: Microsoft					
Product: azure_devops_server					
Affected Version(s): 2020.1.2					
N/A	14-Feb-2023	7.5	Azure DevOps Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21553**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21553	O-MIC-AZUR-270223/2231
Affected Version(s): 2022					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	7.1	Azure DevOps Server Cross-Site Scripting Vulnerability **CVE ID : CVE-2023-21564**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21564	O-MIC-AZUR-270223/2232
Product: windows					
Affected Version(s): -					
N/A	09-Feb-2023	9.8	External Control of Critical State Data, Improper Control of Generation of Code ('Code Injection') vulnerability in YugaByte, Inc. Yugabyte DB on Windows, Linux, MacOS, iOS (DevopsBase.Java:execCommand, TableManager.Java:runCommand modules) allows API Manipulation, Privilege Abuse. This vulnerability is associated with program files backup.Py. This issue affects Yugabyte DB: Lesser then 2.2. **CVE ID : CVE-2023-0575**	N/A	O-MIC-WIND-270223/2233
Improper Neutralization of Special Elements used in an SQL	15-Feb-2023	9.8	Priority Windows may allow Command Execution via SQL Injection using an unspecified method. **CVE ID : CVE-2023-23459**	N/A	O-MIC-WIND-270223/2234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')					
Improper Control of Generation of Code ('Code Injection')	03-Feb-2023	9.8	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system with a specially crafted sequence of serialized objects. IBM X-Force ID: 245513. **CVE ID : CVE-2023-23477**	https://www.ibm.com/support/pages/node/6891111, https://exchange.xforce.ibmcloud.com/vulnerabilities/245513	O-MIC-WIND-270223/2235
Improper Privilege Management	03-Feb-2023	8.4	VMware Workstation contains an arbitrary file deletion vulnerability. A malicious actor with local user privileges on the victim's machine may exploit this vulnerability to delete arbitrary files from the file system of the machine on which Workstation is installed. **CVE ID : CVE-2023-20854**	https://www.vmware.com/security/advisories/VMSA-2023-0003.html	O-MIC-WIND-270223/2236
Uncontrolled Search Path Element	02-Feb-2023	8.2	The protection bypass vulnerability in DLP for Windows 11.9.x is addressed in version 11.10.0. This allowed a local user to bypass DLP controls when uploading sensitive data from a mapped drive into a web email client. Loading from a	https://kcm.trellix.com/corporate/index?page=content&id=SB10394&locale=en_US	O-MIC-WIND-270223/2237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local driver was correctly prevented. Versions prior to 11.9 correctly detected and blocked the attempted upload of sensitive data. **CVE ID : CVE-2023-0400**		
N/A	08-Feb-2023	7.8	A problem with a protection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices allows a local user to execute privileged cytool commands that disable or uninstall the agent. **CVE ID : CVE-2023-0002**	https://security.paloaltonetworks.com/CVE-2023-0002	O-MIC-WIND-270223/2238
Untrusted Search Path	15-Feb-2023	7.8	Untrusted search path vulnerability in ELECOM Camera Assistant 1.00 and QuickFileDealer Ver.1.2.1 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2023-22368**	https://www.elecom.co.jp/news/security/20230214-01/	O-MIC-WIND-270223/2239
Cleartext Transmission of Sensitive Information	08-Feb-2023	6.7	An information exposure vulnerability in the Palo Alto Networks Cortex XDR agent on Windows devices allows a local system administrator to disclose the admin password for the agent in cleartext, which bad	https://security.paloaltonetworks.com/CVE-2023-0001	O-MIC-WIND-270223/2240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			actors can then use to execute privileged cytool commands that disable or uninstall the agent. **CVE ID : CVE-2023-0001**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-2023	4.6	IBM Infosphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 245423. **CVE ID : CVE-2023-23475**	https://www.ibm.com/support/pages/node/6890711	O-MIC-WIND-270223/2241
Product: windows_10					
Affected Version(s): * Up to (excluding) 10.0.10240.19747					
N/A	14-Feb-2023	9.8	Windows iSCSI Discovery Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21803**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21803	O-MIC-WIND-270223/2242
N/A	14-Feb-2023	8.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21695**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21695	O-MIC-WIND-270223/2243
N/A	14-Feb-2023	7.8	Microsoft PostScript Printer Driver Remote	https://msrc.microsoft.co	O-MIC-WIND-270223/2244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-21801**	m/update-guide/vulnerability/CVE-2023-21801	
N/A	14-Feb-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-21802**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21802	O-MIC-WIND-270223/2245
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21804**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21804	O-MIC-WIND-270223/2246
N/A	14-Feb-2023	7.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2023-21805**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21805	O-MIC-WIND-270223/2247
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21812**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812	O-MIC-WIND-270223/2248
N/A	14-Feb-2023	7.8	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21817**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21817	O-MIC-WIND-270223/2249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21822**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21822	O-MIC-WIND-270223/2250
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376	O-MIC-WIND-270223/2251
N/A	14-Feb-2023	7.5	Windows iSCSI Discovery Service Denial of Service Vulnerability **CVE ID : CVE-2023-21700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21700	O-MIC-WIND-270223/2252
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability **CVE ID : CVE-2023-21701**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21701	O-MIC-WIND-270223/2253
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21702**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21702	O-MIC-WIND-270223/2254
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21811**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21811	O-MIC-WIND-270223/2255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21813**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21813	O-MIC-WIND-270223/2256
N/A	14-Feb-2023	7.5	Windows Active Directory Domain Services API Denial of Service Vulnerability **CVE ID : CVE-2023-21816**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21816	O-MIC-WIND-270223/2257
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21818**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21818	O-MIC-WIND-270223/2258
N/A	14-Feb-2023	7.4	Windows Distributed File System (DFS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21820**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21820	O-MIC-WIND-270223/2259
N/A	14-Feb-2023	6.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21694	O-MIC-WIND-270223/2260
N/A	14-Feb-2023	5.7	Microsoft PostScript Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-21693**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21693	O-MIC-WIND-270223/2261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	5.5	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21697**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21697	O-MIC-WIND-270223/2262
N/A	14-Feb-2023	5.3	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21699	O-MIC-WIND-270223/2263
Product: windows_10_1507					
Affected Version(s): * Up to (excluding) 10.0.10240.19747					
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21689**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689	O-MIC-WIND-270223/2264
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690	O-MIC-WIND-270223/2265
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692	O-MIC-WIND-270223/2266
N/A	14-Feb-2023	8.8	Microsoft PostScript Printer Driver Remote	https://msrc.microsoft.com/update-	O-MIC-WIND-270223/2267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-21684**	guide/vulnerability/CVE-2023-21684	
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21685**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21685	O-MIC-WIND-270223/2268
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21686**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21686	O-MIC-WIND-270223/2269
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21797**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21797	O-MIC-WIND-270223/2270
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21798**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21798	O-MIC-WIND-270223/2271
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21799**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21799	O-MIC-WIND-270223/2272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.8	NT OS Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21688**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21688	O-MIC-WIND-270223/2273
N/A	14-Feb-2023	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2023-21823**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21823	O-MIC-WIND-270223/2274
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability **CVE ID : CVE-2023-21691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	O-MIC-WIND-270223/2275
Affected Version(s): *					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2276
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2277
Product: windows_10_1511					
Affected Version(s): *					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-270223/2278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21808	guide/vulnerability/CVE-2023-21808	
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2279
Product: windows_10_1607					
Affected Version(s): -					
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2280
Affected Version(s): *					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2281
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2282
Affected Version(s): * Up to (excluding) 10.0.14393.5717					
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21689**	-2023-21689	
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690	O-MIC-WIND-270223/2284
N/A	14-Feb-2023	9.8	Windows iSCSI Discovery Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21803**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21803	O-MIC-WIND-270223/2285
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692	O-MIC-WIND-270223/2286
N/A	14-Feb-2023	8.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21684**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21684	O-MIC-WIND-270223/2287
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21685**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21685	O-MIC-WIND-270223/2288
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL	https://msrc.microsoft.co	O-MIC-WIND-270223/2289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21686**	m/update-guide/vulnerability/CVE-2023-21686	
N/A	14-Feb-2023	8.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21695**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21695	O-MIC-WIND-270223/2290
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21799**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21799	O-MIC-WIND-270223/2291
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21797**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21797	O-MIC-WIND-270223/2292
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21798**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21798	O-MIC-WIND-270223/2293
N/A	14-Feb-2023	7.8	NT OS Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21688**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21688	O-MIC-WIND-270223/2294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21801**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21801	O-MIC-WIND-270223/2295
N/A	14-Feb-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-21802**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21802	O-MIC-WIND-270223/2296
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21804**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21804	O-MIC-WIND-270223/2297
N/A	14-Feb-2023	7.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2023-21805**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21805	O-MIC-WIND-270223/2298
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21812**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812	O-MIC-WIND-270223/2299
N/A	14-Feb-2023	7.8	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21817**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21817	O-MIC-WIND-270223/2300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21822**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21822	O-MIC-WIND-270223/2301
N/A	14-Feb-2023	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2023-21823**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21823	O-MIC-WIND-270223/2302
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376	O-MIC-WIND-270223/2303
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability **CVE ID : CVE-2023-21691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	O-MIC-WIND-270223/2304
N/A	14-Feb-2023	7.5	Windows iSCSI Discovery Service Denial of Service Vulnerability **CVE ID : CVE-2023-21700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21700	O-MIC-WIND-270223/2305
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21701	O-MIC-WIND-270223/2306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21701		
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21702**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21702	O-MIC-WIND-270223/2307
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21811**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21811	O-MIC-WIND-270223/2308
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21813**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21813	O-MIC-WIND-270223/2309
N/A	14-Feb-2023	7.5	Windows Active Directory Domain Services API Denial of Service Vulnerability **CVE ID : CVE-2023-21816**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21816	O-MIC-WIND-270223/2310
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21818**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21818	O-MIC-WIND-270223/2311
N/A	14-Feb-2023	7.4	Windows Distributed File System (DFS) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21820	-2023-21820	
N/A	14-Feb-2023	6.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21694	O-MIC-WIND-270223/2313
N/A	14-Feb-2023	5.7	Microsoft PostScript Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-21693**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21693	O-MIC-WIND-270223/2314
N/A	14-Feb-2023	5.5	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21697**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21697	O-MIC-WIND-270223/2315
N/A	14-Feb-2023	5.3	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21699	O-MIC-WIND-270223/2316
Product: windows_10_1703					
Affected Version(s): *					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2318
Product: windows_10_1709					
Affected Version(s): *					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2319
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2320
Product: windows_10_1803					
Affected Version(s): *					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2321
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2322
Product: windows_10_1807					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): *					
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2323
Product: windows_10_1809					
Affected Version(s): -					
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2324
Affected Version(s): *					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2325
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2326
Affected Version(s): * Up to (excluding) 10.0.17763.4010					
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21689**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689	O-MIC-WIND-270223/2327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690	O-MIC-WIND-270223/2328
N/A	14-Feb-2023	9.8	Windows iSCSI Discovery Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21803**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21803	O-MIC-WIND-270223/2329
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692	O-MIC-WIND-270223/2330
N/A	14-Feb-2023	8.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21684**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21684	O-MIC-WIND-270223/2331
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21685**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21685	O-MIC-WIND-270223/2332
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21686**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21686	
N/A	14-Feb-2023	8.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21695**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21695	O-MIC-WIND-270223/2334
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21799**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21799	O-MIC-WIND-270223/2335
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21797**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21797	O-MIC-WIND-270223/2336
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21798**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21798	O-MIC-WIND-270223/2337
N/A	14-Feb-2023	7.8	NT OS Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21688**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21688	O-MIC-WIND-270223/2338
N/A	14-Feb-2023	7.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21801	-2023-21801	
N/A	14-Feb-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-21802**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21802	O-MIC-WIND-270223/2340
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21804**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21804	O-MIC-WIND-270223/2341
N/A	14-Feb-2023	7.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2023-21805**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21805	O-MIC-WIND-270223/2342
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21812**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812	O-MIC-WIND-270223/2343
N/A	14-Feb-2023	7.8	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21817**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21817	O-MIC-WIND-270223/2344
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21822	-2023-21822	
N/A	14-Feb-2023	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2023-21823**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21823	O-MIC-WIND-270223/2346
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376	O-MIC-WIND-270223/2347
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability **CVE ID : CVE-2023-21691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	O-MIC-WIND-270223/2348
N/A	14-Feb-2023	7.5	Windows iSCSI Discovery Service Denial of Service Vulnerability **CVE ID : CVE-2023-21700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21700	O-MIC-WIND-270223/2349
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability **CVE ID : CVE-2023-21701**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21701	O-MIC-WIND-270223/2350
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulne	O-MIC-WIND-270223/2351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21702	rability/CVE-2023-21702	
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21811**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21811	O-MIC-WIND-270223/2352
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21813**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21813	O-MIC-WIND-270223/2353
N/A	14-Feb-2023	7.5	Windows Active Directory Domain Services API Denial of Service Vulnerability **CVE ID : CVE-2023-21816**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21816	O-MIC-WIND-270223/2354
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21818**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21818	O-MIC-WIND-270223/2355
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21819**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21819	O-MIC-WIND-270223/2356
N/A	14-Feb-2023	7.4	Windows Distributed File System (DFS) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulne	O-MIC-WIND-270223/2357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21820	rability/CVE-2023-21820	
N/A	14-Feb-2023	6.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21694	O-MIC-WIND-270223/2358
N/A	14-Feb-2023	5.7	Microsoft PostScript Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-21693**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21693	O-MIC-WIND-270223/2359
N/A	14-Feb-2023	5.5	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21697**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21697	O-MIC-WIND-270223/2360
N/A	14-Feb-2023	5.3	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21699	O-MIC-WIND-270223/2361
Product: windows_10_1903					
Affected Version(s): *					
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: windows_10_1909					
Affected Version(s): *					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2363
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2364
Product: windows_10_2004					
Affected Version(s): *					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2365
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2366
Product: windows_10_20h2					
Affected Version(s): *					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21808	
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2368
Affected Version(s): * Up to (excluding) 10.0.19042.2604					
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21689**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689	O-MIC-WIND-270223/2369
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690	O-MIC-WIND-270223/2370
N/A	14-Feb-2023	9.8	Windows iSCSI Discovery Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21803**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21803	O-MIC-WIND-270223/2371
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692	O-MIC-WIND-270223/2372
N/A	14-Feb-2023	8.8	Microsoft PostScript Printer Driver Remote	https://msrc.microsoft.com/update-	O-MIC-WIND-270223/2373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-21684**	guide/vulnerability/CVE-2023-21684	
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21685**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21685	O-MIC-WIND-270223/2374
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21686**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21686	O-MIC-WIND-270223/2375
N/A	14-Feb-2023	8.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21695**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21695	O-MIC-WIND-270223/2376
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21799**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21799	O-MIC-WIND-270223/2377
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21797**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21797	O-MIC-WIND-270223/2378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21798**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21798	O-MIC-WIND-270223/2379
N/A	14-Feb-2023	7.8	NT OS Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21688**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21688	O-MIC-WIND-270223/2380
N/A	14-Feb-2023	7.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21801**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21801	O-MIC-WIND-270223/2381
N/A	14-Feb-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-21802**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21802	O-MIC-WIND-270223/2382
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21804**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21804	O-MIC-WIND-270223/2383
N/A	14-Feb-2023	7.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2023-21805**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21805	O-MIC-WIND-270223/2384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21812**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812	O-MIC-WIND-270223/2385
N/A	14-Feb-2023	7.8	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21817**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21817	O-MIC-WIND-270223/2386
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21822**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21822	O-MIC-WIND-270223/2387
N/A	14-Feb-2023	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2023-21823**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21823	O-MIC-WIND-270223/2388
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376	O-MIC-WIND-270223/2389
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability **CVE ID : CVE-2023-21691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	O-MIC-WIND-270223/2390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.5	Windows iSCSI Discovery Service Denial of Service Vulnerability **CVE ID : CVE-2023-21700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21700	O-MIC-WIND-270223/2391
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability **CVE ID : CVE-2023-21701**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21701	O-MIC-WIND-270223/2392
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21702**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21702	O-MIC-WIND-270223/2393
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21811**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21811	O-MIC-WIND-270223/2394
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21813**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21813	O-MIC-WIND-270223/2395
N/A	14-Feb-2023	7.5	Windows Active Directory Domain Services API Denial of Service Vulnerability **CVE ID : CVE-2023-21816**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21816	O-MIC-WIND-270223/2396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21818**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21818	O-MIC-WIND-270223/2397
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21819**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21819	O-MIC-WIND-270223/2398
N/A	14-Feb-2023	7.4	Windows Distributed File System (DFS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21820**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21820	O-MIC-WIND-270223/2399
N/A	14-Feb-2023	6.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21694	O-MIC-WIND-270223/2400
N/A	14-Feb-2023	5.7	Microsoft PostScript Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-21693**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21693	O-MIC-WIND-270223/2401
N/A	14-Feb-2023	5.5	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21697**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21697	O-MIC-WIND-270223/2402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	5.3	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21699	O-MIC-WIND-270223/2403
Product: windows_10_21h1					
Affected Version(s): *					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2404
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2405
Product: windows_10_21h2					
Affected Version(s): *					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2406
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2407
Affected Version(s): * Up to (excluding) 10.0.19044.2604					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21689**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689	O-MIC-WIND-270223/2408
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690	O-MIC-WIND-270223/2409
N/A	14-Feb-2023	9.8	Windows iSCSI Discovery Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21803**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21803	O-MIC-WIND-270223/2410
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692	O-MIC-WIND-270223/2411
N/A	14-Feb-2023	8.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21684**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21684	O-MIC-WIND-270223/2412
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21685**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21685	
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21686**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21686	O-MIC-WIND-270223/2414
N/A	14-Feb-2023	8.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21695**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21695	O-MIC-WIND-270223/2415
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21799**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21799	O-MIC-WIND-270223/2416
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21797**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21797	O-MIC-WIND-270223/2417
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21798**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21798	O-MIC-WIND-270223/2418
N/A	14-Feb-2023	7.8	NT OS Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21688	-2023-21688	
N/A	14-Feb-2023	7.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21801**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21801	O-MIC-WIND-270223/2420
N/A	14-Feb-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-21802**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21802	O-MIC-WIND-270223/2421
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21804**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21804	O-MIC-WIND-270223/2422
N/A	14-Feb-2023	7.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2023-21805**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21805	O-MIC-WIND-270223/2423
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21812**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812	O-MIC-WIND-270223/2424
N/A	14-Feb-2023	7.8	Windows Kerberos Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21817	-2023-21817	
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21822**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21822	O-MIC-WIND-270223/2426
N/A	14-Feb-2023	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2023-21823**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21823	O-MIC-WIND-270223/2427
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376	O-MIC-WIND-270223/2428
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability **CVE ID : CVE-2023-21691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	O-MIC-WIND-270223/2429
N/A	14-Feb-2023	7.5	Windows iSCSI Discovery Service Denial of Service Vulnerability **CVE ID : CVE-2023-21700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21700	O-MIC-WIND-270223/2430
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(PEAP) Denial of Service Vulnerability **CVE ID : CVE-2023-21701**	-2023-21701	
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21702**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21702	O-MIC-WIND-270223/2432
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21811**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21811	O-MIC-WIND-270223/2433
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21813**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21813	O-MIC-WIND-270223/2434
N/A	14-Feb-2023	7.5	Windows Active Directory Domain Services API Denial of Service Vulnerability **CVE ID : CVE-2023-21816**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21816	O-MIC-WIND-270223/2435
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21818**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21818	O-MIC-WIND-270223/2436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21819**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21819	O-MIC-WIND-270223/2437
N/A	14-Feb-2023	7.4	Windows Distributed File System (DFS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21820**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21820	O-MIC-WIND-270223/2438
N/A	14-Feb-2023	6.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21694	O-MIC-WIND-270223/2439
N/A	14-Feb-2023	5.7	Microsoft PostScript Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-21693**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21693	O-MIC-WIND-270223/2440
N/A	14-Feb-2023	5.5	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21697**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21697	O-MIC-WIND-270223/2441
N/A	14-Feb-2023	5.3	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21699	O-MIC-WIND-270223/2442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21699		
Product: windows_10_22h2					
Affected Version(s): *					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2443
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2444
Affected Version(s): * Up to (excluding) 10.0.19045.2604					
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21689**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689	O-MIC-WIND-270223/2445
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690	O-MIC-WIND-270223/2446
N/A	14-Feb-2023	9.8	Windows iSCSI Discovery Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21803**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21803	O-MIC-WIND-270223/2447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692	O-MIC-WIND-270223/2448
N/A	14-Feb-2023	8.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21684**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21684	O-MIC-WIND-270223/2449
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21685**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21685	O-MIC-WIND-270223/2450
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21686**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21686	O-MIC-WIND-270223/2451
N/A	14-Feb-2023	8.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21695**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21695	O-MIC-WIND-270223/2452
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21799**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21799	
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21797**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21797	O-MIC-WIND-270223/2454
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21798**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21798	O-MIC-WIND-270223/2455
N/A	14-Feb-2023	7.8	NT OS Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21688**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21688	O-MIC-WIND-270223/2456
N/A	14-Feb-2023	7.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21801**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21801	O-MIC-WIND-270223/2457
N/A	14-Feb-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-21802**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21802	O-MIC-WIND-270223/2458
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21804	-2023-21804	
N/A	14-Feb-2023	7.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2023-21805**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21805	O-MIC-WIND-270223/2460
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21812**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812	O-MIC-WIND-270223/2461
N/A	14-Feb-2023	7.8	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21817**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21817	O-MIC-WIND-270223/2462
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21822**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21822	O-MIC-WIND-270223/2463
N/A	14-Feb-2023	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2023-21823**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21823	O-MIC-WIND-270223/2464
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23376	-2023-23376	
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability **CVE ID : CVE-2023-21691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	O-MIC-WIND-270223/2466
N/A	14-Feb-2023	7.5	Windows iSCSI Discovery Service Denial of Service Vulnerability **CVE ID : CVE-2023-21700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21700	O-MIC-WIND-270223/2467
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability **CVE ID : CVE-2023-21701**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21701	O-MIC-WIND-270223/2468
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21702**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21702	O-MIC-WIND-270223/2469
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21811**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21811	O-MIC-WIND-270223/2470
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulne	O-MIC-WIND-270223/2471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21813	rability/CVE-2023-21813	
N/A	14-Feb-2023	7.5	Windows Active Directory Domain Services API Denial of Service Vulnerability **CVE ID : CVE-2023-21816**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21816	O-MIC-WIND-270223/2472
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21818**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21818	O-MIC-WIND-270223/2473
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21819**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21819	O-MIC-WIND-270223/2474
N/A	14-Feb-2023	7.4	Windows Distributed File System (DFS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21820**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21820	O-MIC-WIND-270223/2475
N/A	14-Feb-2023	6.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21694	O-MIC-WIND-270223/2476
N/A	14-Feb-2023	5.7	Microsoft PostScript Printer Driver Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulne	O-MIC-WIND-270223/2477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21693	rability/CVE-2023-21693	
N/A	14-Feb-2023	5.5	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21697**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21697	O-MIC-WIND-270223/2478
N/A	14-Feb-2023	5.3	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21699	O-MIC-WIND-270223/2479
Product: windows_11_21h2					
Affected Version(s): *					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2480
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2481
Affected Version(s): * Up to (excluding) 10.0.22000.1574					
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21690	-2023-21690	
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692	O-MIC-WIND-270223/2483
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21689**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689	O-MIC-WIND-270223/2484
N/A	14-Feb-2023	8.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21684**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21684	O-MIC-WIND-270223/2485
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21685**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21685	O-MIC-WIND-270223/2486
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21686**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21686	O-MIC-WIND-270223/2487
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulne	O-MIC-WIND-270223/2488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21799	rability/CVE-2023-21799	
N/A	14-Feb-2023	8.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21695**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21695	O-MIC-WIND-270223/2489
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21797**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21797	O-MIC-WIND-270223/2490
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21798**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21798	O-MIC-WIND-270223/2491
N/A	14-Feb-2023	7.8	NT OS Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21688**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21688	O-MIC-WIND-270223/2492
N/A	14-Feb-2023	7.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21801**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21801	O-MIC-WIND-270223/2493
N/A	14-Feb-2023	7.8	Windows Media Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulne	O-MIC-WIND-270223/2494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21802	rability/CVE-2023-21802	
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21804**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21804	O-MIC-WIND-270223/2495
N/A	14-Feb-2023	7.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2023-21805**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21805	O-MIC-WIND-270223/2496
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21812**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812	O-MIC-WIND-270223/2497
N/A	14-Feb-2023	7.8	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21817**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21817	O-MIC-WIND-270223/2498
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21822**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21822	O-MIC-WIND-270223/2499
N/A	14-Feb-2023	7.8	Windows Graphics Component Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulne	O-MIC-WIND-270223/2500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21823	rability/CVE-2023-21823	
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376	O-MIC-WIND-270223/2501
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability **CVE ID : CVE-2023-21691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	O-MIC-WIND-270223/2502
N/A	14-Feb-2023	7.5	Windows iSCSI Discovery Service Denial of Service Vulnerability **CVE ID : CVE-2023-21700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21700	O-MIC-WIND-270223/2503
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability **CVE ID : CVE-2023-21701**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21701	O-MIC-WIND-270223/2504
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21702**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21702	O-MIC-WIND-270223/2505
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-270223/2506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21811	guide/vulnerability/CVE-2023-21811	
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21813**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21813	O-MIC-WIND-270223/2507
N/A	14-Feb-2023	7.5	Windows Active Directory Domain Services API Denial of Service Vulnerability **CVE ID : CVE-2023-21816**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21816	O-MIC-WIND-270223/2508
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21818**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21818	O-MIC-WIND-270223/2509
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21819**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21819	O-MIC-WIND-270223/2510
N/A	14-Feb-2023	7.4	Windows Distributed File System (DFS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21820**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21820	O-MIC-WIND-270223/2511
N/A	14-Feb-2023	6.8	Windows Fax Service Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-270223/2512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21694	guide/vulnerability/CVE-2023-21694	
N/A	14-Feb-2023	5.7	Microsoft PostScript Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-21693**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21693	O-MIC-WIND-270223/2513
Exposure of Resource to Wrong Sphere	14-Feb-2023	5.5	HTTP.sys Information Disclosure Vulnerability **CVE ID : CVE-2023-21687**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21687	O-MIC-WIND-270223/2514
Product: windows_11_22h2					
Affected Version(s): *					
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2515
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2516
Affected Version(s): * Up to (excluding) 10.0.22621.1265					
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21689	-2023-21689	
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690	O-MIC-WIND-270223/2518
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692	O-MIC-WIND-270223/2519
N/A	14-Feb-2023	8.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21684**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21684	O-MIC-WIND-270223/2520
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21685**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21685	O-MIC-WIND-270223/2521
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21686**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21686	O-MIC-WIND-270223/2522
N/A	14-Feb-2023	8.8	Microsoft Protected Extensible Authentication Protocol	https://msrc.microsoft.com/update-guide/vulne	O-MIC-WIND-270223/2523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21695**	rability/CVE-2023-21695	
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21797**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21797	O-MIC-WIND-270223/2524
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21798**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21798	O-MIC-WIND-270223/2525
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21799**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21799	O-MIC-WIND-270223/2526
N/A	14-Feb-2023	7.8	NT OS Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21688**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21688	O-MIC-WIND-270223/2527
N/A	14-Feb-2023	7.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21801**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21801	O-MIC-WIND-270223/2528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-21802**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21802	O-MIC-WIND-270223/2529
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21804**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21804	O-MIC-WIND-270223/2530
N/A	14-Feb-2023	7.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2023-21805**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21805	O-MIC-WIND-270223/2531
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21812**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812	O-MIC-WIND-270223/2532
N/A	14-Feb-2023	7.8	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21817**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21817	O-MIC-WIND-270223/2533
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21822**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21822	O-MIC-WIND-270223/2534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2023-21823**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21823	O-MIC-WIND-270223/2535
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376	O-MIC-WIND-270223/2536
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability **CVE ID : CVE-2023-21691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	O-MIC-WIND-270223/2537
N/A	14-Feb-2023	7.5	Windows iSCSI Discovery Service Denial of Service Vulnerability **CVE ID : CVE-2023-21700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21700	O-MIC-WIND-270223/2538
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability **CVE ID : CVE-2023-21701**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21701	O-MIC-WIND-270223/2539
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21702**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21702	
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21811**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21811	O-MIC-WIND-270223/2541
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21813**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21813	O-MIC-WIND-270223/2542
N/A	14-Feb-2023	7.5	Windows Active Directory Domain Services API Denial of Service Vulnerability **CVE ID : CVE-2023-21816**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21816	O-MIC-WIND-270223/2543
N/A	14-Feb-2023	7.4	Windows Distributed File System (DFS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21820**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21820	O-MIC-WIND-270223/2544
N/A	14-Feb-2023	6.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21694	O-MIC-WIND-270223/2545
N/A	14-Feb-2023	5.7	Microsoft PostScript Printer Driver Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21693	-2023-21693	
Exposure of Resource to Wrong Sphere	14-Feb-2023	5.5	HTTP.sys Information Disclosure Vulnerability **CVE ID : CVE-2023-21687**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21687	O-MIC-WIND-270223/2547
Product: windows_server_2008					
Affected Version(s): -					
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21689**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689	O-MIC-WIND-270223/2548
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690	O-MIC-WIND-270223/2549
N/A	14-Feb-2023	9.8	Windows iSCSI Discovery Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21803**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21803	O-MIC-WIND-270223/2550
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692	O-MIC-WIND-270223/2551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	8.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21684**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21684	O-MIC-WIND-270223/2552
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21685**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21685	O-MIC-WIND-270223/2553
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21686**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21686	O-MIC-WIND-270223/2554
N/A	14-Feb-2023	8.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21695**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21695	O-MIC-WIND-270223/2555
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21798**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21798	O-MIC-WIND-270223/2556
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21799**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21799	O-MIC-WIND-270223/2557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21797**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21797	O-MIC-WIND-270223/2558
N/A	14-Feb-2023	7.8	NT OS Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21688**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21688	O-MIC-WIND-270223/2559
N/A	14-Feb-2023	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21800**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21800	O-MIC-WIND-270223/2560
N/A	14-Feb-2023	7.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21801**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21801	O-MIC-WIND-270223/2561
N/A	14-Feb-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-21802**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21802	O-MIC-WIND-270223/2562
N/A	14-Feb-2023	7.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2023-21805**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21805	O-MIC-WIND-270223/2563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2564
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21812**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812	O-MIC-WIND-270223/2565
N/A	14-Feb-2023	7.8	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21817**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21817	O-MIC-WIND-270223/2566
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21822**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21822	O-MIC-WIND-270223/2567
N/A	14-Feb-2023	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2023-21823**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21823	O-MIC-WIND-270223/2568
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376	O-MIC-WIND-270223/2569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability **CVE ID : CVE-2023-21691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	O-MIC-WIND-270223/2570
N/A	14-Feb-2023	7.5	Windows iSCSI Discovery Service Denial of Service Vulnerability **CVE ID : CVE-2023-21700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21700	O-MIC-WIND-270223/2571
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability **CVE ID : CVE-2023-21701**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21701	O-MIC-WIND-270223/2572
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21702**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21702	O-MIC-WIND-270223/2573
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21811**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21811	O-MIC-WIND-270223/2574
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21813**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21813	
N/A	14-Feb-2023	7.5	Windows Active Directory Domain Services API Denial of Service Vulnerability **CVE ID : CVE-2023-21816**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21816	O-MIC-WIND-270223/2576
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21818**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21818	O-MIC-WIND-270223/2577
N/A	14-Feb-2023	7.4	Windows Distributed File System (DFS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21820**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21820	O-MIC-WIND-270223/2578
N/A	14-Feb-2023	6.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21694	O-MIC-WIND-270223/2579
N/A	14-Feb-2023	5.7	Microsoft PostScript Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-21693**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21693	O-MIC-WIND-270223/2580
N/A	14-Feb-2023	5.5	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21697	-2023-21697	
N/A	14-Feb-2023	5.3	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21699	O-MIC-WIND-270223/2582
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2583
Affected Version(s): r2					
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692	O-MIC-WIND-270223/2584
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21689**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689	O-MIC-WIND-270223/2585
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690	O-MIC-WIND-270223/2586
N/A	14-Feb-2023	8.8	Microsoft PostScript Printer Driver Remote	https://msrc.microsoft.co	O-MIC-WIND-270223/2587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-21684**	m/update-guide/vulnerability/CVE-2023-21684	
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21685**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21685	O-MIC-WIND-270223/2588
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21686**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21686	O-MIC-WIND-270223/2589
N/A	14-Feb-2023	8.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21695**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21695	O-MIC-WIND-270223/2590
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21797**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21797	O-MIC-WIND-270223/2591
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21798**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21798	O-MIC-WIND-270223/2592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21799**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21799	O-MIC-WIND-270223/2593
N/A	14-Feb-2023	7.8	NT OS Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21688**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21688	O-MIC-WIND-270223/2594
N/A	14-Feb-2023	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21800**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21800	O-MIC-WIND-270223/2595
N/A	14-Feb-2023	7.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21801**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21801	O-MIC-WIND-270223/2596
N/A	14-Feb-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-21802**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21802	O-MIC-WIND-270223/2597
N/A	14-Feb-2023	7.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2023-21805**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21805	O-MIC-WIND-270223/2598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2599
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21812**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812	O-MIC-WIND-270223/2600
N/A	14-Feb-2023	7.8	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21817**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21817	O-MIC-WIND-270223/2601
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21822**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21822	O-MIC-WIND-270223/2602
N/A	14-Feb-2023	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2023-21823**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21823	O-MIC-WIND-270223/2603
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376	O-MIC-WIND-270223/2604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability **CVE ID : CVE-2023-21691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	O-MIC-WIND-270223/2605
N/A	14-Feb-2023	7.5	Windows iSCSI Discovery Service Denial of Service Vulnerability **CVE ID : CVE-2023-21700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21700	O-MIC-WIND-270223/2606
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability **CVE ID : CVE-2023-21701**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21701	O-MIC-WIND-270223/2607
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21702**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21702	O-MIC-WIND-270223/2608
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21811**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21811	O-MIC-WIND-270223/2609
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21813**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21813	
N/A	14-Feb-2023	7.5	Windows Active Directory Domain Services API Denial of Service Vulnerability **CVE ID : CVE-2023-21816**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21816	O-MIC-WIND-270223/2611
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21818**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21818	O-MIC-WIND-270223/2612
N/A	14-Feb-2023	7.4	Windows Distributed File System (DFS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21820**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21820	O-MIC-WIND-270223/2613
N/A	14-Feb-2023	6.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21694	O-MIC-WIND-270223/2614
N/A	14-Feb-2023	5.7	Microsoft PostScript Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-21693**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21693	O-MIC-WIND-270223/2615
N/A	14-Feb-2023	5.5	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21697	-2023-21697	
N/A	14-Feb-2023	5.3	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21699	O-MIC-WIND-270223/2617
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2618
Product: windows_server_2012					
Affected Version(s): -					
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692	O-MIC-WIND-270223/2619
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21689**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689	O-MIC-WIND-270223/2620
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690	O-MIC-WIND-270223/2621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	8.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21684**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21684	O-MIC-WIND-270223/2622
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21685**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21685	O-MIC-WIND-270223/2623
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21686**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21686	O-MIC-WIND-270223/2624
N/A	14-Feb-2023	8.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21695**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21695	O-MIC-WIND-270223/2625
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21797**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21797	O-MIC-WIND-270223/2626
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21798**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21798	O-MIC-WIND-270223/2627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21799**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21799	O-MIC-WIND-270223/2628
N/A	14-Feb-2023	7.8	NT OS Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21688**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21688	O-MIC-WIND-270223/2629
N/A	14-Feb-2023	7.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21801**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21801	O-MIC-WIND-270223/2630
N/A	14-Feb-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-21802**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21802	O-MIC-WIND-270223/2631
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21804**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21804	O-MIC-WIND-270223/2632
N/A	14-Feb-2023	7.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2023-21805**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21805	O-MIC-WIND-270223/2633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2634
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21812**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812	O-MIC-WIND-270223/2635
N/A	14-Feb-2023	7.8	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21817**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21817	O-MIC-WIND-270223/2636
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21822**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21822	O-MIC-WIND-270223/2637
N/A	14-Feb-2023	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2023-21823**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21823	O-MIC-WIND-270223/2638
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376	O-MIC-WIND-270223/2639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability **CVE ID : CVE-2023-21691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	O-MIC-WIND-270223/2640
N/A	14-Feb-2023	7.5	Windows iSCSI Discovery Service Denial of Service Vulnerability **CVE ID : CVE-2023-21700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21700	O-MIC-WIND-270223/2641
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability **CVE ID : CVE-2023-21701**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21701	O-MIC-WIND-270223/2642
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21702**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21702	O-MIC-WIND-270223/2643
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21811**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21811	O-MIC-WIND-270223/2644
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21813**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21813	
N/A	14-Feb-2023	7.5	Windows Active Directory Domain Services API Denial of Service Vulnerability **CVE ID : CVE-2023-21816**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21816	O-MIC-WIND-270223/2646
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21818**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21818	O-MIC-WIND-270223/2647
N/A	14-Feb-2023	7.4	Windows Distributed File System (DFS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21820**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21820	O-MIC-WIND-270223/2648
N/A	14-Feb-2023	6.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21694	O-MIC-WIND-270223/2649
N/A	14-Feb-2023	5.7	Microsoft PostScript Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-21693**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21693	O-MIC-WIND-270223/2650
N/A	14-Feb-2023	5.5	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21697	-2023-21697	
N/A	14-Feb-2023	5.3	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21699	O-MIC-WIND-270223/2652
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2653
Affected Version(s): r2					
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692	O-MIC-WIND-270223/2654
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21689**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689	O-MIC-WIND-270223/2655
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690	O-MIC-WIND-270223/2656
N/A	14-Feb-2023	8.8	Microsoft PostScript Printer Driver Remote	https://msrc.microsoft.co	O-MIC-WIND-270223/2657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-21684**	m/update-guide/vulnerability/CVE-2023-21684	
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21685**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21685	O-MIC-WIND-270223/2658
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21686**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21686	O-MIC-WIND-270223/2659
N/A	14-Feb-2023	8.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21695**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21695	O-MIC-WIND-270223/2660
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21797**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21797	O-MIC-WIND-270223/2661
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21798**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21798	O-MIC-WIND-270223/2662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21799**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21799	O-MIC-WIND-270223/2663
N/A	14-Feb-2023	7.8	NT OS Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21688**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21688	O-MIC-WIND-270223/2664
N/A	14-Feb-2023	7.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21801**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21801	O-MIC-WIND-270223/2665
N/A	14-Feb-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-21802**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21802	O-MIC-WIND-270223/2666
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21804**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21804	O-MIC-WIND-270223/2667
N/A	14-Feb-2023	7.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2023-21805**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21805	O-MIC-WIND-270223/2668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2669
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21812**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812	O-MIC-WIND-270223/2670
N/A	14-Feb-2023	7.8	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21817**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21817	O-MIC-WIND-270223/2671
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21822**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21822	O-MIC-WIND-270223/2672
N/A	14-Feb-2023	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2023-21823**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21823	O-MIC-WIND-270223/2673
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376	O-MIC-WIND-270223/2674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability **CVE ID : CVE-2023-21691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	O-MIC-WIND-270223/2675
N/A	14-Feb-2023	7.5	Windows iSCSI Discovery Service Denial of Service Vulnerability **CVE ID : CVE-2023-21700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21700	O-MIC-WIND-270223/2676
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability **CVE ID : CVE-2023-21701**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21701	O-MIC-WIND-270223/2677
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21702**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21702	O-MIC-WIND-270223/2678
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21811**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21811	O-MIC-WIND-270223/2679
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21813**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21813	
N/A	14-Feb-2023	7.5	Windows Active Directory Domain Services API Denial of Service Vulnerability **CVE ID : CVE-2023-21816**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21816	O-MIC-WIND-270223/2681
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21818**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21818	O-MIC-WIND-270223/2682
N/A	14-Feb-2023	7.4	Windows Distributed File System (DFS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21820**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21820	O-MIC-WIND-270223/2683
N/A	14-Feb-2023	6.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21694	O-MIC-WIND-270223/2684
N/A	14-Feb-2023	5.7	Microsoft PostScript Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-21693**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21693	O-MIC-WIND-270223/2685
N/A	14-Feb-2023	5.5	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21697	-2023-21697	
N/A	14-Feb-2023	5.3	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21699	O-MIC-WIND-270223/2687
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2688
Product: windows_server_2016					
Affected Version(s): -					
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692	O-MIC-WIND-270223/2689
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21689**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689	O-MIC-WIND-270223/2690
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690	O-MIC-WIND-270223/2691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	8.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21684**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21684	O-MIC-WIND-270223/2692
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21685**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21685	O-MIC-WIND-270223/2693
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21686**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21686	O-MIC-WIND-270223/2694
N/A	14-Feb-2023	8.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21695**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21695	O-MIC-WIND-270223/2695
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21797**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21797	O-MIC-WIND-270223/2696
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21798**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21798	O-MIC-WIND-270223/2697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21799**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21799	O-MIC-WIND-270223/2698
N/A	14-Feb-2023	7.8	NT OS Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21688**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21688	O-MIC-WIND-270223/2699
N/A	14-Feb-2023	7.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21801**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21801	O-MIC-WIND-270223/2700
N/A	14-Feb-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-21802**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21802	O-MIC-WIND-270223/2701
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21804**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21804	O-MIC-WIND-270223/2702
N/A	14-Feb-2023	7.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2023-21805**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21805	O-MIC-WIND-270223/2703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2704
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21812**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812	O-MIC-WIND-270223/2705
N/A	14-Feb-2023	7.8	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21817**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21817	O-MIC-WIND-270223/2706
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21822**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21822	O-MIC-WIND-270223/2707
N/A	14-Feb-2023	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2023-21823**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21823	O-MIC-WIND-270223/2708
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376	O-MIC-WIND-270223/2709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability **CVE ID : CVE-2023-21691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	O-MIC-WIND-270223/2710
N/A	14-Feb-2023	7.5	Windows iSCSI Discovery Service Denial of Service Vulnerability **CVE ID : CVE-2023-21700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21700	O-MIC-WIND-270223/2711
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability **CVE ID : CVE-2023-21701**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21701	O-MIC-WIND-270223/2712
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21702**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21702	O-MIC-WIND-270223/2713
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21811**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21811	O-MIC-WIND-270223/2714
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21813**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21813	
N/A	14-Feb-2023	7.5	Windows Active Directory Domain Services API Denial of Service Vulnerability **CVE ID : CVE-2023-21816**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21816	O-MIC-WIND-270223/2716
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21818**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21818	O-MIC-WIND-270223/2717
N/A	14-Feb-2023	7.4	Windows Distributed File System (DFS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21820**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21820	O-MIC-WIND-270223/2718
N/A	14-Feb-2023	6.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21694	O-MIC-WIND-270223/2719
N/A	14-Feb-2023	5.7	Microsoft PostScript Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-21693**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21693	O-MIC-WIND-270223/2720
N/A	14-Feb-2023	5.5	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21697	-2023-21697	
N/A	14-Feb-2023	5.3	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21699	O-MIC-WIND-270223/2722
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2723
Product: windows_server_2019					
Affected Version(s): -					
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692	O-MIC-WIND-270223/2724
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21689**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689	O-MIC-WIND-270223/2725
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690	O-MIC-WIND-270223/2726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	8.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21684**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21684	O-MIC-WIND-270223/2727
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21685**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21685	O-MIC-WIND-270223/2728
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21686**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21686	O-MIC-WIND-270223/2729
N/A	14-Feb-2023	8.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21695**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21695	O-MIC-WIND-270223/2730
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21797**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21797	O-MIC-WIND-270223/2731
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21798**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21798	O-MIC-WIND-270223/2732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21799**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21799	O-MIC-WIND-270223/2733
N/A	14-Feb-2023	7.8	NT OS Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21688**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21688	O-MIC-WIND-270223/2734
N/A	14-Feb-2023	7.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21801**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21801	O-MIC-WIND-270223/2735
N/A	14-Feb-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-21802**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21802	O-MIC-WIND-270223/2736
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21804**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21804	O-MIC-WIND-270223/2737
N/A	14-Feb-2023	7.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2023-21805**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21805	O-MIC-WIND-270223/2738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2739
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21812**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812	O-MIC-WIND-270223/2740
N/A	14-Feb-2023	7.8	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21817**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21817	O-MIC-WIND-270223/2741
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21822**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21822	O-MIC-WIND-270223/2742
N/A	14-Feb-2023	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2023-21823**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21823	O-MIC-WIND-270223/2743
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376	O-MIC-WIND-270223/2744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability **CVE ID : CVE-2023-21691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	O-MIC-WIND-270223/2745
N/A	14-Feb-2023	7.5	Windows iSCSI Discovery Service Denial of Service Vulnerability **CVE ID : CVE-2023-21700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21700	O-MIC-WIND-270223/2746
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability **CVE ID : CVE-2023-21701**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21701	O-MIC-WIND-270223/2747
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21702**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21702	O-MIC-WIND-270223/2748
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21811**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21811	O-MIC-WIND-270223/2749
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21813**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2023-21813	
N/A	14-Feb-2023	7.5	Windows Active Directory Domain Services API Denial of Service Vulnerability **CVE ID : CVE-2023-21816**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21816	O-MIC-WIND-270223/2751
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21818**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21818	O-MIC-WIND-270223/2752
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21819**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21819	O-MIC-WIND-270223/2753
N/A	14-Feb-2023	7.4	Windows Distributed File System (DFS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21820**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21820	O-MIC-WIND-270223/2754
N/A	14-Feb-2023	6.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-21694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21694	O-MIC-WIND-270223/2755
N/A	14-Feb-2023	5.7	Microsoft PostScript Printer Driver Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21693	-2023-21693	
N/A	14-Feb-2023	5.5	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21697**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21697	O-MIC-WIND-270223/2757
N/A	14-Feb-2023	5.3	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability **CVE ID : CVE-2023-21699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21699	O-MIC-WIND-270223/2758
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2759
Product: windows_server_2022					
Affected Version(s): -					
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690	O-MIC-WIND-270223/2760
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692	O-MIC-WIND-270223/2761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	9.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21689**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689	O-MIC-WIND-270223/2762
N/A	14-Feb-2023	8.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21684**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21684	O-MIC-WIND-270223/2763
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21685**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21685	O-MIC-WIND-270223/2764
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21686**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21686	O-MIC-WIND-270223/2765
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21798**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21798	O-MIC-WIND-270223/2766
N/A	14-Feb-2023	8.8	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21695	O-MIC-WIND-270223/2767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21695		
N/A	14-Feb-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-21799**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21799	O-MIC-WIND-270223/2768
N/A	14-Feb-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21797**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21797	O-MIC-WIND-270223/2769
N/A	14-Feb-2023	7.8	NT OS Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21688**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21688	O-MIC-WIND-270223/2770
N/A	14-Feb-2023	7.8	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-21801**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21801	O-MIC-WIND-270223/2771
N/A	14-Feb-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-21802**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21802	O-MIC-WIND-270223/2772
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21804	-2023-21804	
N/A	14-Feb-2023	7.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2023-21805**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21805	O-MIC-WIND-270223/2774
N/A	14-Feb-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-21808**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21808	O-MIC-WIND-270223/2775
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21812**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812	O-MIC-WIND-270223/2776
N/A	14-Feb-2023	7.8	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21817**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21817	O-MIC-WIND-270223/2777
N/A	14-Feb-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21822**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21822	O-MIC-WIND-270223/2778
N/A	14-Feb-2023	7.8	Windows Graphics Component Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-270223/2779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21823	-2023-21823	
N/A	14-Feb-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376	O-MIC-WIND-270223/2780
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability **CVE ID : CVE-2023-21691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	O-MIC-WIND-270223/2781
N/A	14-Feb-2023	7.5	Windows iSCSI Discovery Service Denial of Service Vulnerability **CVE ID : CVE-2023-21700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21700	O-MIC-WIND-270223/2782
N/A	14-Feb-2023	7.5	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability **CVE ID : CVE-2023-21701**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21701	O-MIC-WIND-270223/2783
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability **CVE ID : CVE-2023-21702**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21702	O-MIC-WIND-270223/2784
N/A	14-Feb-2023	7.5	Windows iSCSI Service Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulne	O-MIC-WIND-270223/2785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21811	rability/CVE-2023-21811	
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21813**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21813	O-MIC-WIND-270223/2786
N/A	14-Feb-2023	7.5	Windows Active Directory Domain Services API Denial of Service Vulnerability **CVE ID : CVE-2023-21816**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21816	O-MIC-WIND-270223/2787
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21818**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21818	O-MIC-WIND-270223/2788
N/A	14-Feb-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-21819**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21819	O-MIC-WIND-270223/2789
N/A	14-Feb-2023	7.4	Windows Distributed File System (DFS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-21820**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21820	O-MIC-WIND-270223/2790
N/A	14-Feb-2023	6.8	Windows Fax Service Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulne	O-MIC-WIND-270223/2791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21694	rability/CVE-2023-21694	
N/A	14-Feb-2023	5.7	Microsoft PostScript Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-21693**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21693	O-MIC-WIND-270223/2792
Exposure of Resource to Wrong Sphere	14-Feb-2023	5.5	HTTP.sys Information Disclosure Vulnerability **CVE ID : CVE-2023-21687**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21687	O-MIC-WIND-270223/2793
N/A	14-Feb-2023	5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2023-21722**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21722	O-MIC-WIND-270223/2794
Vendor: multilaser					
Product: re057_firmware					
Affected Version(s): 2.1					
N/A	03-Feb-2023	7.5	A vulnerability, which was classified as critical, was found in Multilaser RE057 and RE170 2.1/2.2. This affects an unknown part of the file /param.file.tgz of the component Backup File Handler. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The identifier VDB-	N/A	O-MUL-RE05-270223/2795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			220053 was assigned to this vulnerability. **CVE ID : CVE-2023-0658**		
Affected Version(s): 2.2					
N/A	03-Feb-2023	7.5	A vulnerability, which was classified as critical, was found in Multilaser RE057 and RE170 2.1/2.2. This affects an unknown part of the file /param.file.tgz of the component Backup File Handler. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The identifier VDB-220053 was assigned to this vulnerability. **CVE ID : CVE-2023-0658**	N/A	O-MUL-RE05-270223/2796
Product: re170_firmware					
Affected Version(s): 2.1					
N/A	03-Feb-2023	7.5	A vulnerability, which was classified as critical, was found in Multilaser RE057 and RE170 2.1/2.2. This affects an unknown part of the file /param.file.tgz of the component Backup File Handler. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The identifier VDB-	N/A	O-MUL-RE17-270223/2797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			220053 was assigned to this vulnerability. **CVE ID : CVE-2023-0658**		
Affected Version(s): 2.2					
N/A	03-Feb-2023	7.5	A vulnerability, which was classified as critical, was found in Multilaser RE057 and RE170 2.1/2.2. This affects an unknown part of the file /param.file.tgz of the component Backup File Handler. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The identifier VDB-220053 was assigned to this vulnerability. **CVE ID : CVE-2023-0658**	N/A	O-MUL-RE17-270223/2798
Vendor: Netgear					
Product: d6100_firmware					
Affected Version(s): * Up to (including) 1.0.0.63					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and	https://www.netgear.com/about/security/	O-NET-D610-270223/2799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier. **CVE ID : CVE-2023-23110**		
Product: dgn1000v3_firmware					
Affected Version(s): * Up to (including) 1.0.0.22					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum	https://www.netgear.com/about/security/	O-NET-DGN1-270223/2800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier. **CVE ID : CVE-2023-23110**		
Product: prosafe_fs726tp_firmware					
Affected Version(s): -					
Insufficiently Protected Credentials	15-Feb-2023	7.5	An uspecified endpoint in the web server of the switch does not properly authenticate the user identity, and may allow downloading a config page with the password to the switch in clear text. **CVE ID : CVE-2023-24498**	N/A	O-NET-PROS-270223/2801
Product: r8900_firmware					
Affected Version(s): * Up to (including) 1.0.3.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier. **CVE ID : CVE-2023-23110**	https://www.netgear.com/about/security/	O-NET-R890-270223/2802
Product: r9000_firmware					
Affected Version(s): * Up to (including) 1.0.3.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier. **CVE ID : CVE-2023-23110**	https://www.netgear.com/about/security/	O-NET-R900-270223/2803
Product: wndr3700_firmware					
Affected Version(s): 1.0.1.14					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	15-Feb-2023	9.8	A vulnerability has been found in Netgear WNDR3700v2 1.0.1.14 and classified as critical. This vulnerability affects unknown code of the component Web Interface. The manipulation leads to command injection. 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-221152. **CVE ID : CVE-2023-0849**	N/A	O-NET-WNDR-270223/2804
N/A	15-Feb-2023	7.5	A vulnerability was found in Netgear WNDR3700v2 1.0.1.14. It has been rated as problematic. This issue affects some unknown processing of the component Web Management Interface. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221147. **CVE ID : CVE-2023-0848**	N/A	O-NET-WNDR-270223/2805
N/A	15-Feb-2023	7.5	A vulnerability was found in Netgear WNDR3700v2 1.0.1.14	N/A	O-NET-WNDR-270223/2806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and classified as problematic. This issue affects some unknown processing of the component Web Interface. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221153 was assigned to this vulnerability. **CVE ID : CVE-2023-0850**		
Product: wnr1000v2_firmware					
Affected Version(s): * Up to (including) 1.1.2.60					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier,	https://www.netgear.com/about/security/	O-NET-WNR1-270223/2807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier. **CVE ID : CVE-2023-23110**		
Product: wnr2200_firmware					
Affected Version(s): * Up to (including) 1.0.1.102					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless	https://www.netgear.com/about/security/	O-NET-WNR2-270223/2808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier. **CVE ID : CVE-2023-23110**		
Product: wnr2500_firmware					
Affected Version(s): * Up to (including) 1.0.0.34					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and	https://www.netgear.com/about/security/	O-NET-WNR2-270223/2809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, XAVN2001v2 Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier. **CVE ID : CVE-2023-23110**		
Product: wnr612v2_firmware					
Affected Version(s): * Up to (including) 1.0.0.3					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2	https://www.netgear.com/about/security/	O-NET-WNR6-270223/2810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wireless-N Extenders 0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier. **CVE ID : CVE-2023-23110**		
Product: xavn2001v2_firmware					
Affected Version(s): * Up to (including) 0.4.0.7					
Download of Code Without Integrity Check	02-Feb-2023	7.4	An exploitable firmware modification vulnerability was discovered in certain Netgear products. The data integrity of the uploaded firmware image is ensured with a fixed checksum number. Therefore, an attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the checksum verification. This affects WNR612v2 Wireless Routers 1.0.0.3 and earlier, DGN1000v3 Modem Router 1.0.0.22 and earlier, D6100 WiFi DSL Modem Routers 1.0.0.63 and earlier, WNR1000v2 Wireless Routers 1.1.2.60 and earlier, XAVN2001v2 Wireless-N Extenders	https://www.netgear.com/about/security/	O-NET-XAVN-270223/2811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.4.0.7 and earlier, WNR2200 Wireless Routers 1.0.1.102 and earlier, WNR2500 Wireless Routers 1.0.0.34 and earlier, R8900 Smart WiFi Routers 1.0.3.6 and earlier, and R9000 Smart WiFi Routers 1.0.3.6 and earlier. **CVE ID : CVE-2023-23110**		
Vendor: onekey					
Product: onekey_mini_firmware					
Affected Version(s): * Up to (including) 2.10.0					
N/A	14-Feb-2023	4.2	Onekey Touch devices through 4.0.0 and Onekey Mini devices through 2.10.0 allow man-in-the-middle attackers to obtain the seed phase. The man-in-the-middle access can only be obtained after disassembling a device (i.e., here, "man-in-the-middle" does not refer to the attacker's position on an IP network). NOTE: the vendor states that "our hardware team has updated the security patch without anyone being affected." **CVE ID : CVE-2023-25758**	https://blog.onekey.so/our-response-to-recent-security-fix-reports-13914fea8afd	O-ONE-ONEK-270223/2812
Product: onekey_touch_firmware					
Affected Version(s): * Up to (including) 4.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Feb-2023	4.2	Onekey Touch devices through 4.0.0 and Onekey Mini devices through 2.10.0 allow man-in-the-middle attackers to obtain the seed phase. The man-in-the-middle access can only be obtained after disassembling a device (i.e., here, "man-in-the-middle" does not refer to the attacker's position on an IP network). NOTE: the vendor states that "our hardware team has updated the security patch without anyone being affected." **CVE ID : CVE-2023-25758**	https://blog.onekey.so/our-response-to-recent-security-fix-reports-13914fea8afd	O-ONE-ONEK-270223/2813
Vendor: Opensuse					
Product: leap					
Affected Version(s): 15.4					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Feb-2023	7.8	An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in libzypp-plugin-appdata of SUSE Linux Enterprise Server for SAP 15-SP3; openSUSE Leap 15.4 allows attackers that can trick users to use specially crafted REPO_ALIAS, REPO_TYPE or REPO_METADATA_PATH settings to execute	https://bugzilla.suse.com/show_bug.cgi?id=1206836	O-OPE-LEAP-270223/2814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code as root. This issue affects: SUSE Linux Enterprise Server for SAP 15-SP3 libzypp-plugin-appdata versions prior to 1.0.1+git.20180426. openSUSE Leap 15.4 libzypp-plugin-appdata versions prior to 1.0.1+git.20180426. **CVE ID : CVE-2023-22643**		
Vendor: Oracle					
Product: solaris					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	03-Feb-2023	9.8	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system with a specially crafted sequence of serialized objects. IBM X-Force ID: 245513. **CVE ID : CVE-2023-23477**	https://www.ibm.com/support/pages/node/6891111, https://exchange.xforce.ibmcloud.com/vulnerabilities/245513	O-ORA-SOLA-270223/2815
Vendor: Planex					
Product: cs-wmv02g					
Affected Version(s): *					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	5.2	** UNSUPPORTED WHEN ASSIGNED ** Stored cross-site scripting vulnerability in Wired/Wireless LAN Pan/Tilt Network Camera CS-WMV02G all versions allows a network-adjacent authenticated attacker	https://www.planex.co.jp/support/support_end_list.shtml	O-PLA-CS-W-270223/2816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to inject an arbitrary script. NOTE: This vulnerability only affects products that are no longer supported by the developer. **CVE ID : CVE-2023-22370**		
Product: cs-wmv02g_firmware					
Affected Version(s): *					
Cross-Site Request Forgery (CSRF)	14-Feb-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** Cross-site request forgery (CSRF) vulnerability in Wired/Wireless LAN Pan/Tilt Network Camera CS-WMV02G all versions allows a remote unauthenticated attacker to hijack the authentication and conduct arbitrary operations by having a logged-in user to view a malicious page. NOTE: This vulnerability only affects products that are no longer supported by the developer. **CVE ID : CVE-2023-22375**	N/A	O-PLA-CS-W-270223/2817
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Feb-2023	6.1	** UNSUPPORTED WHEN ASSIGNED ** Reflected cross-site scripting vulnerability in Wired/Wireless LAN Pan/Tilt Network Camera CS-WMV02G all versions allows a remote unauthenticated attacker to inject	N/A	O-PLA-CS-W-270223/2818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary script to inject an arbitrary script. NOTE: This vulnerability only affects products that are no longer supported by the developer. **CVE ID : CVE-2023-22376**		
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 8.0					
Observable Discrepancy	15-Feb-2023	7.5	A timing side-channel in the handling of RSA ClientKeyExchange messages was discovered in GnuTLS. This side-channel can be sufficient to recover the key encrypted in the RSA ciphertext across a network in a Bleichenbacher style attack. To achieve a successful decryption the attacker would need to send a large amount of specially crafted messages to the vulnerable server. By recovering the secret from the ClientKeyExchange message, the attacker would be able to decrypt the application data exchanged over that connection. **CVE ID : CVE-2023-0361**	https://gitlab.com/gnutls/gnutls/-/issues/1050, https://github.com/tlsfuzzer/tlsfuzzer/pull/679	O-RED-ENTE-270223/2819
Affected Version(s): 9.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	15-Feb-2023	7.5	A timing side-channel in the handling of RSA ClientKeyExchange messages was discovered in GnuTLS. This side-channel can be sufficient to recover the key encrypted in the RSA ciphertext across a network in a Bleichenbacher style attack. To achieve a successful decryption the attacker would need to send a large amount of specially crafted messages to the vulnerable server. By recovering the secret from the ClientKeyExchange message, the attacker would be able to decrypt the application data exchanged over that connection. **CVE ID : CVE-2023-0361**	https://gitlab.com/gnutls/gnutls/-/issues/1050, https://github.com/tlsfuzzer/tlsfuzzer/pull/679	O-RED-ENTE-270223/2820
Vendor: revolt-power					
Product: inverter_firmware					
Affected Version(s): mw3_15u_5406_1.47					
Use of Hard-coded Credentials	13-Feb-2023	6.8	A vulnerability was found in Deye/Revolt/Bosswerk Inverter MW3_15U_5406_1.47/MW3_15U_5406_1.471. It has been rated as problematic. This issue affects some unknown processing of the component Access	N/A	O-REV-INVE-270223/2821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Point Setting Handler. The manipulation with the input 12345678 leads to use of hard-coded password. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. Upgrading to version MW3_16U_5406_1.53 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-220769 was assigned to this vulnerability. **CVE ID : CVE-2023-0808**		
Affected Version(s): mw3_15u_5406_1.471					
Use of Hard-coded Credentials	13-Feb-2023	6.8	A vulnerability was found in Deye/Revolt/Bosswerk Inverter MW3_15U_5406_1.47/ MW3_15U_5406_1.471. It has been rated as problematic. This issue affects some unknown processing of the component Access Point Setting Handler. The manipulation with the input 12345678 leads to use of hard-coded password. It is possible to launch the attack on the physical device. The exploit has been disclosed to the	N/A	O-REV-INVE-270223/2822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. Upgrading to version MW3_16U_5406_1.53 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-220769 was assigned to this vulnerability. **CVE ID : CVE-2023-0808**		
Vendor: Ruckuswireless					
Product: smartzone					
Affected Version(s): * Up to (excluding) 5.2.1.3					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	O-RUC-SMAR-270223/2823
Affected Version(s): * Up to (excluding) 5.2.1.3.1695					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	O-RUC-SMAR-270223/2824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 6.1.0.0.935					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	O-RUC-SMAR-270223/2825
Product: smartzone_ap					
Affected Version(s): * Up to (excluding) 3.6.2.0.795					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	O-RUC-SMAR-270223/2826
Affected Version(s): * Up to (excluding) 5.2.2.0.2064					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	O-RUC-SMAR-270223/2827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 6.1.0.0.9240					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	O-RUC-SMAR-270223/2828
Affected Version(s): * Up to (excluding) 6.1.1.0.1274					
Improper Control of Generation of Code ('Code Injection')	13-Feb-2023	9.8	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring. **CVE ID : CVE-2023-25717**	https://support.ruckuswireless.com/security_bulletins/315	O-RUC-SMAR-270223/2829
Vendor: Samsung					
Product: android					
Affected Version(s): 10.0					
Use of Externally-Controlled Format String	09-Feb-2023	7.8	Use of Externally-Controlled Format String vulnerabilities in STST TA prior to SMR Jan-2023 Release 1 allows arbitrary code execution. **CVE ID : CVE-2023-21420**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2830
Improper Privilege	09-Feb-2023	7.8	Improper Handling of Insufficient Permissions	https://security.samsung	O-SAM-ANDR-270223/2831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			or Privileges vulnerability in KnoxCustomManagerService prior to SMR Jan-2023 Release 1 allows attacker to access device SIM PIN. **CVE ID : CVE-2023-21421**	mobile.com/securityUpdate.smsb?year=2023&month=01	
Out-of-bounds Read	09-Feb-2023	7.8	An out-of-bound read vulnerability in mapToBuffer function in libSDKRecognitionText.spensdk.samsung.so library prior to SMR JAN-2023 Release 1 allows attacker to cause memory access fault. **CVE ID : CVE-2023-21430**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2832
Improper Authentication	09-Feb-2023	5.5	Improper access control vulnerability in telecom application prior to SMR JAN-2023 Release 1 allows local attackers to get sensitive information. **CVE ID : CVE-2023-21425**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2833
Use of Hard-coded Credentials	09-Feb-2023	5.5	Hardcoded AES key to encrypt cardemulation PINs in NFC prior to SMR Jan-2023 Release 1 allows attackers to access cardemulation PIN. **CVE ID : CVE-2023-21426**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	09-Feb-2023	5.5	Improper access control vulnerability in Phone application prior to SMR Feb-2023 Release 1 allows local attackers to access sensitive information via implicit broadcast. **CVE ID : CVE-2023-21437**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2835
Insufficient Verification of Data Authenticity	09-Feb-2023	5.5	Insufficient Verification of Data Authenticity vulnerability in Routine prior to versions 2.6.30.6 in Android Q(10), 3.1.21.10 in Android R(11) and 3.5.2.23 in Android S(12) allows local attacker to access protected files via unused code. **CVE ID : CVE-2023-21441**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=02	O-SAM-ANDR-270223/2836
N/A	09-Feb-2023	3.3	Improper usage of implict intent in ePDG prior to SMR JAN-2023 Release 1 allows attacker to access SSID. **CVE ID : CVE-2023-21429**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2837
N/A	09-Feb-2023	3.3	Improper usage of implicit intent in Contacts prior to SMR Feb-2023 Release 1 allows attacker to get account ID. **CVE ID : CVE-2023-21436**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2838
Affected Version(s): 11.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	09-Feb-2023	7.8	Use of Externally-Controlled Format String vulnerabilities in STST TA prior to SMR Jan-2023 Release 1 allows arbitrary code execution. **CVE ID : CVE-2023-21420**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2839
Improper Privilege Management	09-Feb-2023	7.8	Improper Handling of Insufficient Permissions or Privileges vulnerability in KnoxCustomManagerService prior to SMR Jan-2023 Release 1 allows attacker to access device SIM PIN. **CVE ID : CVE-2023-21421**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2840
Out-of-bounds Read	09-Feb-2023	7.8	An out-of-bound read vulnerability in mapToBuffer function in libSDKRecognitionText.spensdk.samsung.so library prior to SMR JAN-2023 Release 1 allows attacker to cause memory access fault. **CVE ID : CVE-2023-21430**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2841
Exposure of Resource to Wrong Sphere	09-Feb-2023	7.8	Improper access control vulnerability in MyFiles prior to versions 12.2.09 in Android R(11), 13.1.03.501 in Android S(12) and 14.1.00.422 in Android T(13) allows local attacker to write file with MyFiles	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=02	O-SAM-ANDR-270223/2842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege via implicit intent. **CVE ID : CVE-2023-21445**		
N/A	09-Feb-2023	6.5	Improper access control vulnerability in NfcTile prior to SMR Jan-2023 Release 1 allows to attacker to use NFC without user recognition. **CVE ID : CVE-2023-21427**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2843
Incorrect Authorization	09-Feb-2023	5.5	Improper authorization vulnerability in semAddPublicDnsAddr in WifiSevice prior to SMR Jan-2023 Release 1 allows attackers to set custom DNS server without permission via binding WifiService. **CVE ID : CVE-2023-21422**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2844
Improper Authentication	09-Feb-2023	5.5	Improper access control vulnerability in telecom application prior to SMR JAN-2023 Release 1 allows local attackers to get sensitive information. **CVE ID : CVE-2023-21425**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2845
Insertion of Sensitive Information into Log File	09-Feb-2023	5.5	Exposure of Sensitive Information vulnerability in Fingerprint TA prior to SMR Feb-2023 Release 1 allows attackers to access the memory	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address information via log. **CVE ID : CVE-2023-21435**		
Improper Authentication	09-Feb-2023	5.5	Improper access control vulnerability in Phone application prior to SMR Feb-2023 Release 1 allows local attackers to access sensitive information via implicit broadcast. **CVE ID : CVE-2023-21437**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2847
Insufficient Verification of Data Authenticity	09-Feb-2023	5.5	Insufficient Verification of Data Authenticity vulnerability in Routine prior to versions 2.6.30.6 in Android Q(10), 3.1.21.10 in Android R(11) and 3.5.2.23 in Android S(12) allows local attacker to access protected files via unused code. **CVE ID : CVE-2023-21441**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=02	O-SAM-ANDR-270223/2848
N/A	09-Feb-2023	5.5	Improper access control vulnerability in Runestone application prior to version 2.9.09.003 in Android R(11) and 3.2.01.007 in Android S(12) allows local attackers to get device location information. **CVE ID : CVE-2023-21442**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=02	O-SAM-ANDR-270223/2849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-Feb-2023	5.5	Improper input validation in MyFiles prior to version 12.2.09 in Android R(11), 13.1.03.501 in Android S(12) and 14.1.00.422 in Android T(13) allows local attacker to access data of MyFiles. **CVE ID : CVE-2023-21446**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=02	O-SAM-ANDR-270223/2850
Incorrect Authorization	09-Feb-2023	3.3	Improper Handling of Insufficient Permissions or Privileges vulnerability in SemChameleonHelper prior to SMR Jan-2023 Release 1 allows attacker to modify network related values, network code, carrier id and operator brand. **CVE ID : CVE-2023-21424**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2851
Improper Input Validation	09-Feb-2023	3.3	Improper input validation vulnerability in TelephonyUI prior to SMR Jan-2023 Release 1 allows attackers to configure Preferred Call. The patch removes unused code. **CVE ID : CVE-2023-21428**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2852
N/A	09-Feb-2023	3.3	Improper usage of implict intent in ePDG prior to SMR JAN-2023 Release 1 allows attacker to access SSID. **CVE ID : CVE-2023-21429**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Feb-2023	3.3	Improper usage of implicit intent in Contacts prior to SMR Feb-2023 Release 1 allows attacker to get account ID. **CVE ID : CVE-2023-21436**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2854
Exposure of Resource to Wrong Sphere	09-Feb-2023	2.4	Improper logic in HomeScreen prior to SMR Feb-2023 Release 1 allows physical attacker to access App preview protected by Secure Folder. **CVE ID : CVE-2023-21438**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2855
Affected Version(s): 12.0					
Improper Privilege Management	09-Feb-2023	7.8	Improper Handling of Insufficient Permissions or Privileges vulnerability in KnoxCustomManagerService prior to SMR Jan-2023 Release 1 allows attacker to access device SIM PIN. **CVE ID : CVE-2023-21421**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2856
Out-of-bounds Read	09-Feb-2023	7.8	An out-of-bound read vulnerability in mapToBuffer function in libSDKRecognitionText.spensdk.samsung.so library prior to SMR JAN-2023 Release 1 allows attacker to cause memory access fault. **CVE ID : CVE-2023-21430**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-Feb-2023	7.8	Improper input validation vulnerability in UwbDataTxStatusEvent prior to SMR Feb-2023 Release 1 allows attackers to launch certain activities. **CVE ID : CVE-2023-21439**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2858
Exposure of Resource to Wrong Sphere	09-Feb-2023	7.8	Improper access control vulnerability in MyFiles prior to versions 12.2.09 in Android R(11), 13.1.03.501 in Android S(12) and 14.1.00.422 in Android T(13) allows local attacker to write file with MyFiles privilege via implicit intent. **CVE ID : CVE-2023-21445**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=02	O-SAM-ANDR-270223/2859
Out-of-bounds Write	09-Feb-2023	7.8	A Stack-based overflow vulnerability in IpcRxEmbmsSessionList in SECRIL prior to Android S(12) allows attacker to cause memory corruptions. **CVE ID : CVE-2023-21451**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=04	O-SAM-ANDR-270223/2860
N/A	09-Feb-2023	6.5	Improper access control vulnerability in NfcTile prior to SMR Jan-2023 Release 1 allows to attacker to use NFC without user recognition.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21427		
Incorrect Authorization	09-Feb-2023	5.5	Improper authorization vulnerability in semAddPublicDnsAddr in WifiSevice prior to SMR Jan-2023 Release 1 allows attackers to set custom DNS server without permission via binding WifiService. **CVE ID : CVE-2023-21422**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2862
Incorrect Authorization	09-Feb-2023	5.5	Improper authorization vulnerability in ChnFileShareKit prior to SMR Jan-2023 Release 1 allows attacker to control BLE advertising without permission using unprotected action. **CVE ID : CVE-2023-21423**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2863
Improper Authentication	09-Feb-2023	5.5	Improper access control vulnerability in telecom application prior to SMR JAN-2023 Release 1 allows local attackers to get sensitive information. **CVE ID : CVE-2023-21425**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2864
Insertion of Sensitive Information into Log File	09-Feb-2023	5.5	Exposure of Sensitive Information vulnerability in Fingerprint TA prior to SMR Feb-2023 Release 1 allows attackers to access the memory	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address information via log. **CVE ID : CVE-2023-21435**		
Improper Authentication	09-Feb-2023	5.5	Improper access control vulnerability in Phone application prior to SMR Feb-2023 Release 1 allows local attackers to access sensitive information via implicit broadcast. **CVE ID : CVE-2023-21437**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2866
Insufficient Verification of Data Authenticity	09-Feb-2023	5.5	Insufficient Verification of Data Authenticity vulnerability in Routine prior to versions 2.6.30.6 in Android Q(10), 3.1.21.10 in Android R(11) and 3.5.2.23 in Android S(12) allows local attacker to access protected files via unused code. **CVE ID : CVE-2023-21441**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=02	O-SAM-ANDR-270223/2867
N/A	09-Feb-2023	5.5	Improper access control vulnerability in Runestone application prior to version 2.9.09.003 in Android R(11) and 3.2.01.007 in Android S(12) allows local attackers to get device location information. **CVE ID : CVE-2023-21442**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=02	O-SAM-ANDR-270223/2868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-Feb-2023	5.5	Improper input validation in MyFiles prior to version 12.2.09 in Android R(11), 13.1.03.501 in Android S(12) and 14.1.00.422 in Android T(13) allows local attacker to access data of MyFiles. **CVE ID : CVE-2023-21446**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=02	O-SAM-ANDR-270223/2869
Incorrect Authorization	09-Feb-2023	3.3	Improper Handling of Insufficient Permissions or Privileges vulnerability in SemChameleonHelper prior to SMR Jan-2023 Release 1 allows attacker to modify network related values, network code, carrier id and operator brand. **CVE ID : CVE-2023-21424**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2870
Improper Input Validation	09-Feb-2023	3.3	Improper input validation vulnerability in TelephonyUI prior to SMR Jan-2023 Release 1 allows attackers to configure Preferred Call. The patch removes unused code. **CVE ID : CVE-2023-21428**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2871
N/A	09-Feb-2023	3.3	Improper usage of implict intent in ePDG prior to SMR JAN-2023 Release 1 allows attacker to access SSID. **CVE ID : CVE-2023-21429**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Feb-2023	3.3	Improper usage of implicit intent in Contacts prior to SMR Feb-2023 Release 1 allows attacker to get account ID. **CVE ID : CVE-2023-21436**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2873
Exposure of Resource to Wrong Sphere	09-Feb-2023	2.4	Improper logic in HomeScreen prior to SMR Feb-2023 Release 1 allows physical attacker to access App preview protected by Secure Folder. **CVE ID : CVE-2023-21438**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2874
Affected Version(s): 13.0					
Improper Privilege Management	09-Feb-2023	7.8	Improper Handling of Insufficient Permissions or Privileges vulnerability in KnoxCustomManagerService prior to SMR Jan-2023 Release 1 allows attacker to access device SIM PIN. **CVE ID : CVE-2023-21421**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2875
Out-of-bounds Read	09-Feb-2023	7.8	An out-of-bound read vulnerability in mapToBuffer function in libSDKRecognitionText.spensdk.samsung.so library prior to SMR JAN-2023 Release 1 allows attacker to cause memory access fault. **CVE ID : CVE-2023-21430**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-Feb-2023	7.8	Improper input validation vulnerability in UwbDataTxStatusEvent prior to SMR Feb-2023 Release 1 allows attackers to launch certain activities. **CVE ID : CVE-2023-21439**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2877
Exposure of Resource to Wrong Sphere	09-Feb-2023	7.8	Improper access control vulnerability in MyFiles prior to versions 12.2.09 in Android R(11), 13.1.03.501 in Android S(12) and 14.1.00.422 in Android T(13) allows local attacker to write file with MyFiles privilege via implicit intent. **CVE ID : CVE-2023-21445**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=02	O-SAM-ANDR-270223/2878
N/A	09-Feb-2023	6.5	Improper access control vulnerability in NfcTile prior to SMR Jan-2023 Release 1 allows to attacker to use NFC without user recognition. **CVE ID : CVE-2023-21427**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2879
Incorrect Authorization	09-Feb-2023	5.5	Improper authorization vulnerability in ChnFileShareKit prior to SMR Jan-2023 Release 1 allows attacker to control BLE advertising without permission using unprotected action.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21423		
Improper Authentication	09-Feb-2023	5.5	Improper access control vulnerability in telecom application prior to SMR JAN-2023 Release 1 allows local attackers to get sensitive information. **CVE ID : CVE-2023-21425**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2881
Insertion of Sensitive Information into Log File	09-Feb-2023	5.5	Exposure of Sensitive Information vulnerability in Fingerprint TA prior to SMR Feb-2023 Release 1 allows attackers to access the memory address information via log. **CVE ID : CVE-2023-21435**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2882
Improper Authentication	09-Feb-2023	5.5	Improper access control vulnerability in Phone application prior to SMR Feb-2023 Release 1 allows local attackers to access sensitive information via implicit broadcast. **CVE ID : CVE-2023-21437**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2883
Inclusion of Functionality from Untrusted Control Sphere	09-Feb-2023	5.5	Improper access control vulnerability in WindowManagerService prior to SMR Feb-2023 Release 1 allows attackers to take a screen capture. **CVE ID : CVE-2023-21440**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-Feb-2023	5.5	Improper input validation in MyFiles prior to version 12.2.09 in Android R(11), 13.1.03.501 in Android S(12) and 14.1.00.422 in Android T(13) allows local attacker to access data of MyFiles. **CVE ID : CVE-2023-21446**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=02	O-SAM-ANDR-270223/2885
Incorrect Authorization	09-Feb-2023	3.3	Improper Handling of Insufficient Permissions or Privileges vulnerability in SemChameleonHelper prior to SMR Jan-2023 Release 1 allows attacker to modify network related values, network code, carrier id and operator brand. **CVE ID : CVE-2023-21424**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2886
Improper Input Validation	09-Feb-2023	3.3	Improper input validation vulnerability in TelephonyUI prior to SMR Jan-2023 Release 1 allows attackers to configure Preferred Call. The patch removes unused code. **CVE ID : CVE-2023-21428**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2887
N/A	09-Feb-2023	3.3	Improper usage of implict intent in ePDG prior to SMR JAN-2023 Release 1 allows attacker to access SSID. **CVE ID : CVE-2023-21429**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=01	O-SAM-ANDR-270223/2888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Feb-2023	3.3	Improper usage of implicit intent in Contacts prior to SMR Feb-2023 Release 1 allows attacker to get account ID. **CVE ID : CVE-2023-21436**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=02	O-SAM-ANDR-270223/2889
Vendor: sunellsecurity					
Product: sn-adr3804e1_firmware					
Affected Version(s): -					
Insufficiently Protected Credentials	15-Feb-2023	7.5	Sunell DVR, latest version, Insufficiently Protected Credentials (CWE-522) may be exposed through an unspecified request. **CVE ID : CVE-2023-23463**	N/A	O-SUN-SN-A-270223/2890
N/A	15-Feb-2023	6.5	Sunell DVR, latest version, CWE-200: Exposure of Sensitive Information to an Unauthorized Actor through an unspecified request. **CVE ID : CVE-2023-23458**	N/A	O-SUN-SN-A-270223/2891
Product: sn-adr3808e1_firmware					
Affected Version(s): -					
Insufficiently Protected Credentials	15-Feb-2023	7.5	Sunell DVR, latest version, Insufficiently Protected Credentials (CWE-522) may be exposed through an unspecified request. **CVE ID : CVE-2023-23463**	N/A	O-SUN-SN-A-270223/2892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	15-Feb-2023	6.5	Sunell DVR, latest version, CWE-200: Exposure of Sensitive Information to an Unauthorized Actor through an unspecified request. **CVE ID : CVE-2023-23458**	N/A	O-SUN-SN-A-270223/2893
Product: sn-adr3808e2_firmware					
Affected Version(s): -					
Insufficiently Protected Credentials	15-Feb-2023	7.5	Sunell DVR, latest version, Insufficiently Protected Credentials (CWE-522) may be exposed through an unspecified request. **CVE ID : CVE-2023-23463**	N/A	O-SUN-SN-A-270223/2894
N/A	15-Feb-2023	6.5	Sunell DVR, latest version, CWE-200: Exposure of Sensitive Information to an Unauthorized Actor through an unspecified request. **CVE ID : CVE-2023-23458**	N/A	O-SUN-SN-A-270223/2895
Product: sn-adr3816e1_firmware					
Affected Version(s): -					
Insufficiently Protected Credentials	15-Feb-2023	7.5	Sunell DVR, latest version, Insufficiently Protected Credentials (CWE-522) may be exposed through an unspecified request. **CVE ID : CVE-2023-23463**	N/A	O-SUN-SN-A-270223/2896
N/A	15-Feb-2023	6.5	Sunell DVR, latest version, CWE-200:	N/A	O-SUN-SN-A-270223/2897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exposure of Sensitive Information to an Unauthorized Actor through an unspecified request. **CVE ID : CVE-2023-23458**		
Product: sn-adr3816e2_firmware					
Affected Version(s): -					
Insufficiently Protected Credentials	15-Feb-2023	7.5	Sunell DVR, latest version, Insufficiently Protected Credentials (CWE-522) may be exposed through an unspecified request. **CVE ID : CVE-2023-23463**	N/A	O-SUN-SN-A-270223/2898
N/A	15-Feb-2023	6.5	Sunell DVR, latest version, CWE-200: Exposure of Sensitive Information to an Unauthorized Actor through an unspecified request. **CVE ID : CVE-2023-23458**	N/A	O-SUN-SN-A-270223/2899
Product: sn-xvr3804e1_firmware					
Affected Version(s): -					
Insufficiently Protected Credentials	15-Feb-2023	7.5	Sunell DVR, latest version, Insufficiently Protected Credentials (CWE-522) may be exposed through an unspecified request. **CVE ID : CVE-2023-23463**	N/A	O-SUN-SN-X-270223/2900
N/A	15-Feb-2023	6.5	Sunell DVR, latest version, CWE-200: Exposure of Sensitive Information to an	N/A	O-SUN-SN-X-270223/2901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Unauthorized Actor through an unspecified request. **CVE ID : CVE-2023-23458**		
Product: sn-xvr3808e2_firmware					
Affected Version(s): -					
Insufficiently Protected Credentials	15-Feb-2023	7.5	Sunell DVR, latest version, Insufficiently Protected Credentials (CWE-522) may be exposed through an unspecified request. **CVE ID : CVE-2023-23463**	N/A	O-SUN-SN-X-270223/2902
N/A	15-Feb-2023	6.5	Sunell DVR, latest version, CWE-200: Exposure of Sensitive Information to an Unauthorized Actor through an unspecified request. **CVE ID : CVE-2023-23458**	N/A	O-SUN-SN-X-270223/2903
Vendor: Suse					
Product: suse_linux_enterprise_server					
Affected Version(s): 15					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Feb-2023	7.8	An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in libzypp-plugin-appdata of SUSE Linux Enterprise Server for SAP 15-SP3; openSUSE Leap 15.4 allows attackers that can trick users to use specially crafted	https://bugzilla.suse.com/show_bug.cgi?id=1206836	O-SUS-SUSE-270223/2904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			REPO_ALIAS, REPO_TYPE or REPO_METADATA_PATH settings to execute code as root. This issue affects: SUSE Linux Enterprise Server for SAP 15-SP3 libzypp-plugin-appdata versions prior to 1.0.1+git.20180426. openSUSE Leap 15.4 libzypp-plugin-appdata versions prior to 1.0.1+git.20180426. **CVE ID : CVE-2023-22643**		
Vendor: Tenda					
Product: ac23_firmware					
Affected Version(s): 16.03.07.45					
Out-of-bounds Write	11-Feb-2023	9.8	A vulnerability was found in Tenda AC23 16.03.07.45 and classified as critical. Affected by this issue is the function formSetSysToolDDNS/formGetSysToolDDNS of the file /bin/httpd. The manipulation leads to out-of-bounds write. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-220640. **CVE ID : CVE-2023-0782**	N/A	O-TEN-AC23-270223/2905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: totolink					
Product: a7100ru_firmware					
Affected Version(s): 7.4cu.2313_b20191024					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Feb-2023	9.8	TOTOlink A7100RU(V7.4cu.2313_B20191024) was discovered to contain a command injection vulnerability via the country parameter at setting/delStaticDhcpRules. **CVE ID : CVE-2023-24276**	N/A	O-TOT-A710-270223/2906
Product: ca300-poe_firmware					
Affected Version(s): 6.2c.884					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the host_time parameter in the NTPSyncWithHost function. **CVE ID : CVE-2023-24138**	N/A	O-TOT-CA30-270223/2907
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the NetDiagHost parameter in the setNetworkDiag function. **CVE ID : CVE-2023-24139**	N/A	O-TOT-CA30-270223/2908
Improper Neutralization of Special	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection	N/A	O-TOT-CA30-270223/2909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			vulnerability via the NetDiagPingNum parameter in the setNetworkDiag function. **CVE ID : CVE-2023-24140**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the NetDiagPingTimeOut parameter in the setNetworkDiag function. **CVE ID : CVE-2023-24141**	N/A	O-TOT-CA30-270223/2910
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the NetDiagPingSize parameter in the setNetworkDiag function. **CVE ID : CVE-2023-24142**	N/A	O-TOT-CA30-270223/2911
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the NetDiagTracertHop parameter in the setNetworkDiag function. **CVE ID : CVE-2023-24143**	N/A	O-TOT-CA30-270223/2912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the hour parameter in the setRebootScheCfg function. **CVE ID : CVE-2023-24144**	N/A	O-TOT-CA30-270223/2913
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the plugin_version parameter in the setUnloadUserData function. **CVE ID : CVE-2023-24145**	N/A	O-TOT-CA30-270223/2914
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the minute parameter in the setRebootScheCfg function. **CVE ID : CVE-2023-24146**	N/A	O-TOT-CA30-270223/2915
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the FileName parameter in the setUploadUserData function. **CVE ID : CVE-2023-24148**	N/A	O-TOT-CA30-270223/2916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	03-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a hard code password for root which is stored in the component /etc/shadow. **CVE ID : CVE-2023-24149**	N/A	O-TOT-CA30-270223/2917
Improper Neutralization of Special Elements used in a Command ('Command Injection')	14-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the admpass parameter in the setPasswordCfg function. **CVE ID : CVE-2023-24159**	N/A	O-TOT-CA30-270223/2918
Improper Neutralization of Special Elements used in a Command ('Command Injection')	14-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the admuser parameter in the setPasswordCfg function. **CVE ID : CVE-2023-24160**	N/A	O-TOT-CA30-270223/2919
Improper Neutralization of Special Elements used in a Command ('Command Injection')	14-Feb-2023	9.8	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the webWlanIdx parameter in the setWebWlanIdx function. **CVE ID : CVE-2023-24161**	N/A	O-TOT-CA30-270223/2920
Use of Hard-	03-Feb-2023	7.5	TOTOLINK CA300-PoE V6.2c.884 was	N/A	O-TOT-CA30-270223/2921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			discovered to contain a hard code password for the telnet service which is stored in the component /etc/config/product.ini. **CVE ID : CVE-2023-24147**		
Product: t8_firmware					
Affected Version(s): v4.1.5cu					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	A command injection vulnerability in the serverIp parameter in the function meshSlaveDlfw of TOTOLINK T8 V4.1.5cu allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2023-24150**	N/A	O-TOT-T8_F-270223/2922
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	A command injection vulnerability in the ip parameter in the function recvSlaveCloudCheckStatus of TOTOLINK T8 V4.1.5cu allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2023-24151**	N/A	O-TOT-T8_F-270223/2923
Improper Neutralization of Special Elements used in a Command	03-Feb-2023	9.8	A command injection vulnerability in the serverIp parameter in the function meshSlaveUpdate of TOTOLINK T8 V4.1.5cu allows attackers to	N/A	O-TOT-T8_F-270223/2924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2023-24152**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	A command injection vulnerability in the version parameter in the function recvSlaveCloudCheckStatus of TOTOLINK T8 V4.1.5cu allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2023-24153**	N/A	O-TOT-T8_F-270223/2925
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	TOTOLINK T8 V4.1.5cu was discovered to contain a command injection vulnerability via the slaveIpList parameter in the function setUpgradeFW. **CVE ID : CVE-2023-24154**	N/A	O-TOT-T8_F-270223/2926
Use of Hard-coded Credentials	03-Feb-2023	9.8	TOTOLINK T8 V4.1.5cu was discovered to contain a hard code password for the telnet service which is stored in the component /web_cste/cgi-bin/product.ini. **CVE ID : CVE-2023-24155**	N/A	O-TOT-T8_F-270223/2927
Improper Neutralization of Special	03-Feb-2023	9.8	A command injection vulnerability in the ip parameter in the function	N/A	O-TOT-T8_F-270223/2928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			recvSlaveUpgstatus of TOTOLINK T8 V4.1.5cu allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2023-24156**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-2023	9.8	A command injection vulnerability in the serverIp parameter in the function updateWifiInfo of TOTOLINK T8 V4.1.5cu allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2023-24157**	N/A	O-TOT-T8_F-270223/2929
Vendor: Trendnet					
Product: tew-652brp_firmware					
Affected Version(s): 3.04b01					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Feb-2023	9.8	A vulnerability was found in TRENDnet TEW-652BRP 3.04b01. It has been classified as critical. Affected is an unknown function of the file ping.ccp of the component Web Interface. The manipulation leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this	N/A	O-TRE-TEW--270223/2930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-220020. **CVE ID : CVE-2023-0640**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Feb-2023	8.8	A vulnerability, which was classified as critical, has been found in TRENDnet TEW-652BRP 3.04B01. This issue affects some unknown processing of the file get_set.ccp of the component Web Management Interface. The manipulation leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-219935. **CVE ID : CVE-2023-0611**	N/A	O-TRE-TEW--270223/2931
Out-of-bounds Write	01-Feb-2023	7.5	A vulnerability was found in TRENDnet TEW-652BRP 3.04B01. It has been declared as critical. This vulnerability affects unknown code of the file cfg_op.ccp of the component Web Service. The manipulation leads to memory corruption. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-	N/A	O-TRE-TEW--270223/2932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			219958 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0618**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Feb-2023	6.1	A vulnerability was found in TRENDnet TEW-652BRP 3.04b01 and classified as problematic. This issue affects some unknown processing of the file get_set.ccp of the component Web Management Interface. The manipulation of the argument nextPage leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-220019. **CVE ID : CVE-2023-0639**	N/A	O-TRE-TEW--270223/2933
Product: tew-811dru_firmware					
Affected Version(s): 1.0.10.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Feb-2023	9.8	A vulnerability has been found in TRENDnet TEW-811DRU 1.0.10.0 and classified as critical. This vulnerability affects unknown code of the component Web Interface. The manipulation leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to	N/A	O-TRE-TEW--270223/2934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. VDB-220018 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0638**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	A vulnerability, which was classified as critical, was found in TRENDnet TEW-811DRU 1.0.10.0. Affected is an unknown function of the file /wireless/basic.asp of the component httpd. The manipulation leads to 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-219936. **CVE ID : CVE-2023-0612**	N/A	O-TRE-TEW--270223/2935
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Feb-2023	7.5	A vulnerability has been found in TRENDnet TEW-811DRU 1.0.10.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /wireless/security.asp of the component httpd. The manipulation leads to memory corruption. The attack can be launched remotely. The exploit has been	N/A	O-TRE-TEW--270223/2936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. The identifier VDB-219937 was assigned to this vulnerability. **CVE ID : CVE-2023-0613**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Feb-2023	7.5	A vulnerability was found in TRENDNet TEW-811DRU 1.0.10.0. It has been classified as critical. This affects an unknown part of the file /wireless/guestnetwork.asp of the component httpd. The manipulation leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-219957 was assigned to this vulnerability. **CVE ID : CVE-2023-0617**	N/A	O-TRE-TEW--270223/2937
Out-of-bounds Write	02-Feb-2023	6.5	A vulnerability, which was classified as critical, was found in TRENDnet TEW-811DRU 1.0.10.0. This affects an unknown part of the file wan.asp of the component Web Management Interface. The manipulation leads to memory corruption. It is possible to initiate the attack remotely. The exploit has been disclosed to the public	N/A	O-TRE-TEW--270223/2938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and may be used. The identifier VDB-220017 was assigned to this vulnerability. **CVE ID : CVE-2023-0637**		
Product: tv-ip651wi_firmware					
Affected Version(s): * Up to (including) 1.07.01					
Improper Validation of Integrity Check Value	02-Feb-2023	5.9	The use of the cyclic redundancy check (CRC) algorithm for integrity check during firmware update makes TRENDnet TV-IP651WI Network Camera firmware version v1.07.01 and earlier vulnerable to firmware modification attacks. An attacker can conduct a man-in-the-middle (MITM) attack to modify the new firmware image and bypass the checksum verification. **CVE ID : CVE-2023-23120**	https://www.trendnet.com/support/	O-TRE-TV-I-270223/2939
Vendor: ui					
Product: af-2x_firmware					
Affected Version(s): * Up to (excluding) 3.2.2					
Improper Validation of Integrity Check Value	02-Feb-2023	5.9	The use of the cyclic redundancy check (CRC) algorithm for integrity check during firmware update makes Ubiquiti airFiber AF2X Radio firmware version 3.2.2 and earlier vulnerable to firmware modification attacks. An	https://community.ui.com/tags/security/releases	O-UI-AF-2-270223/2940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can conduct a man-in-the-middle (MITM) attack to modify the new firmware image and bypass the checksum verification. **CVE ID : CVE-2023-23119**		
Product: er-10x_firmware					
Affected Version(s): * Up to (excluding) 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-ER-1-270223/2941
Affected Version(s): 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-	O-UI-ER-1-270223/2942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	965a85633b5f	
Product: er-12p_firmware					
Affected Version(s): * Up to (excluding) 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-ER-1-270223/2943
Affected Version(s): 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-	O-UI-ER-1-270223/2944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	965a85633b5f	
Product: er-12_firmware					
Affected Version(s): * Up to (excluding) 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-ER-1-270223/2945
Affected Version(s): 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-ER-1-270223/2946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**		
Product: er-4_firmware					
Affected Version(s): * Up to (excluding) 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-ER-4-270223/2947
Affected Version(s): 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-ER-4-270223/2948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**		
Product: er-6p_firmware					
Affected Version(s): * Up to (excluding) 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-ER-6-270223/2949
Affected Version(s): 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-ER-6-270223/2950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**		
Product: er-8-xg_firmware					
Affected Version(s): * Up to (excluding) 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-ER-8-270223/2951
Affected Version(s): 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-ER-8-270223/2952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**		
Product: er-x-sfp_firmware					
Affected Version(s): * Up to (excluding) 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-ER-X-270223/2953
Affected Version(s): 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-ER-X-270223/2954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**		
Product: er-x_firmware					
Affected Version(s): * Up to (excluding) 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-ER-X-270223/2955
Affected Version(s): 2.0.9					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-ER-X-270223/2956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**		
Product: usg-pro-4_firmware					
Affected Version(s): * Up to (excluding) 4.4.57					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-USG--270223/2957
Product: usg_firmware					
Affected Version(s): * Up to (excluding) 4.4.57					
Improper Control of Generation of Code ('Code Injection')	09-Feb-2023	8.8	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an	https://community.ui.com/releases/Security-Advisory-Bulletin-028-028/696e4e3b-718c-4da4-9a21-965a85633b5f	O-UI-USG_-270223/2958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device to create a remote code execution vulnerability. **CVE ID : CVE-2023-23912**		