National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 - 15 Jul 2022 Vol. 09 No. 13

Table of Content

Vendor	Product	Page Number
Application		
aceattorneyonline	akashi	1
adminite	adminlte	1
admin_management_xtended_project	admin_management_xtended	2
agilepoint	agilepoint_nx	3
anuvaad-corpus_project	anuvaad-corpus	3
Apache	commons_configuration	3
	druid	5
appfire	jira_misc_custom_fields	5
audio_aligner_app_project	audio_aligner_app	6
automatedquizeval_project	automatedquizeval	6
automox	automox	6
averta	shortcodes_and_extra_features_for_phlox_theme	7
awin	awin_data_feed	7
baiduwenkuspider_flaskweb_project	baiduwenkuspider_flaskweb	8
barry_voice_assistant_project	barry_voice_assistant	8
beego	beego	9
bold-themes	bold_page_builder	9
bonn_activity_maps_annotation_tool_project	bonn_activity_maps_annotation_tool	10
bt_lnmp_project	bt_lnmp	10
carceresbe_project	carceresbe	10
caretakerr-api_project	caretakerr-api	11
ceneo-web-scrapper_project	ceneo-web-scrapper	11
chafa_project	chafa	12
chainer	chainerrl-visualizer	12

Vendor	Product	Page Number
changepop-back_project	changepop-back	12
Checkpoint	endpoint_security	13
	harmony_endpoint	15
Cisco	expressway	17
	smart_software_manager_on-prem	18
	telepresence_collaboration_endpoint	19
	telepresence_video_communication_server	20
	unified_communications_manager	22
	unified_communications_manager_im_and_presence_service	31
	unity_connection	39
citeum	opencti	43
clinic\'s_patient_management_system_project	clinic\'s_patient_management_system	44
CMU	opendiamond	45
cockybook_project	cockybook	45
Codesys	opc_da_server	46
Codologic	codoforum	46
college_management_system_project	college_management_system	46
comment_license_project	comment_license	47
control-webpanel	webpanel	47
csm_server_project	csm_server	48
cuyz	valinor	48
Cybozu	garoon	49
dainst	cilantro	55
data_stream_algorithm_benchmark_project	data_stream_algorithm_benchmark	55
deep_learning_studio_project	deep_learning_studio	56
Dell	cloud_mobility_for_dell_emc_storage	56
	powerprotect_cyber_recovery	56
denx	u-boot	57
devolutions	devolutions_server	58

Vendor	Product	Page Number
dice_project	dice	58
digitalguardian	digital_guardian	59
Djangoproject	django	59
Eclipse	jetty	60
Elastic	endpoint_security	64
	kibana	64
eqs	integrity_line	65
equanimity_project	equanimity	65
fan_platform_project	fan_platform	66
fishtank_project	fishtank	66
flask-file-server_project	flask-file-server	67
flask-mongo-skel_project	flask-mongo-skel	67
flask-mvc_project	flask-mvc	67
flask-yeoman_project	flask-yeoman	68
foxy-shop	foxyshop	68
gallagher	command_centre	68
ganga_project	ganga	73
getoutline	outline	73
git-clone_project	git-clone	73
Gitlab	gitlab	74
glance_project	glance	95
Gnupg	gnupg	96
golem_project	golem	96
H3C	ssl_vpn	96
harveyzyh_python_project	harveyzyh_python	97
Haxx	curl	97
hcltechsw	hcl_launch	100
helm-flask-celery_project	helm-flask-celery	101
heroiclabs	nakama	101
Hex-rays	ida	102
hin-eng-preprocessing_project	hin-eng-preprocessing	102
homepage_project	homepage	103

Vendor	Product	Page Number
home__internet_project	home__internet	103
hongcms_project	hongcms	104
hospital_management_system_project	hospital_management_system	104
hotel_management_system_project	hotel_management_system	105
Humhub	humhub	106
hyperledger	fabric	108
iasset_project	iasset	109
IBM	app_connect_enterprise_certified_container	109
	cics_tx	110
	infosphere_information_server	111
	open_liberty	112
	security_verify_access	112
	urbancode_deploy	117
	websphere_application_server	119
idayrus	e-voting	120
iedadata	usap-dc_web_submission_and_dataset_search	120
ingredient_stock_management_system_project	ingredient_stock_management_system	120
internshipsystem_project	internshipsystem	121
Iobit	advanced_systemcare	121
	advanced_system_care	122
	driver_booster	124
	itop_screenshot	124
	itop_screen_recorder	125
	itop_vpn	126
Jetbrains	hub	127
joinbookwyrm	bookwyrm	128
jpegoptim_project	jpegoptim	128
jsrsasign_project	jsrsasign	129

Vendor	Product	Page Number
karaokey_project	karaokey	129
kg-fashion-chatbot_project	kg-fashion-chatbot	130
kitestudio	core_plugin_for_kitestudio_themes	130
kotekan_project	kotekan	131
krypton_project	krypton	131
libmobi_project	libmobi	131
link-preview-js_project	link-preview-js	132
Linuxfoundation	kubeedge	132
Litecart	litecart	152
livro_python_project	livro_python	153
logstash-management-api_project	logstash-management-api	153
LUA	lua	154
Lxml	lxml	154
Magnolia-cms	magnolia_cms	155
Mariadb	mariadb	156
Maxfoundry	wp-paginate	167
md2roff_project	md2roff	167
mdweb_project	mdweb	167
Mediawiki	mediawiki	168
mercadoenlineaback_project	mercadoenlineaback	171
mercury_sample_manager_project	mercury_sample_manager	171
Microsoft	edge_chromium	172
Microweber	microweber	172
mingsoft	mcms	173
mini_tmall_project	mini_tmall	174
modelconverter_project	modelconverter	174
momentjs	moment	174
monorepo_project	monorepo	175
mosaic_project	mosaic	176
movie-review-sentiment-analysis_project	movie-review-sentiment-analysis	176
mp-m08-interface_project	mp-m08-interface	177

Vendor	Product	Page Number
munhak	munhak-moa	177
nesote	inout_homestay	177
newsletter_module_project	newsletter_module	178
nextauth.js	next-auth	178
Nextcloud	nextcloud_mail	181
	nextcloud_server	183
ninjateam	wp_duplicate_page	188
northern.tech	mender	189
nurse_quest_project	nurse_quest	193
Nvidia	nvflare	193
Omron	sysmac_studio	194
online_accreditation_management_system_project	online_accreditation_management_system	196
onyxforum_project	onyxforum	197
openssh_key_parser_project	openssh_key_parser	197
Openssl	openssl	198
Openvpn	openvpn_access_server	200
orchest	orchest	201
otfcc_project	otfcc	201
paddlepaddle	anakin	201
pagebar_project	pagebar	202
parity	frontier	202
passport_project	passport	204
pdfalto_project	pdfalto	204
photo_tag_project	photo_tag	204
portswigger	burp_suite	205
priority-software	priority	205
projects_project	projects	206
purestorage	pure_swagger	207
python-flask-restful-api_project	python-flask-restful-api	207
python-recipe-database_project	python-recipe-database	208
pythonweb_project	pythonweb	208
python_athena_stack_project	python_athena_stack	208

Vendor	Product	Page Number
quic-go_project	quic-go	209
realestate_project	realestate	209
Redhat	keycloak	210
redirection-for-contact-form7	redirection_for_contact_form_7	210
rename_wp-login_project	rename_wp-login	211
rexians	rex-web	211
roxy-wi	roxy-wi	212
rpc.py_project	rpc.py	213
s3label_project	s3label	214
Samsung	find_my_mobile	214
	galaxy_store	214
	samsung_gallery	215
SAP	businessobjects_business_intelligence_platform	216
	businessobjects_bw_publisher_service	218
	business_objects_business_intelligence_platform	218
	business_one	219
	enterprise_extension_defense_forces_\&_public_security	219
scorelab	openmf	224
scss-tokenizer_project	scss-tokenizer	225
setupbox_project	setupbox	225
shackerpanel_project	shackerpanel	225
sharebar_project	sharebar	226
shiva-server_project	shiva-server	226
shortcut_macros_project	shortcut_macros	227
Siemens	pads_viewer	227
	simcenter_femap	236
simple-rat_project	simple-rat	237
simple_parking_management_system_project	simple_parking_management_system	237

Vendor	Product	Page Number
simple_sales_management_system_project	simple_sales_management_system	238
sleep_learner_project	sleep_learner	239
snipeitapp	snipe-it	239
soflyy	wp_all_import	240
solar-system-simulator_project	solar-system-simulator	241
so_filter_shop_by_project	so_filter_shop_by	241
sphere_imagebackend_project	sphere_imagebackend	241
sphere_project	sphere	242
sygnoos	popup_builder	242
Synology	calendar	243
	photo_station	243
syntactics	free_booking_plugin_for_hotels\,_restaurant_and_car_rental	244
syrabond_project	syrabond	244
testplatform_project	testplatform	245
themeisle	wp_maintenance_mode_\&_coming_soon	245
thinkst	canarytokens	245
thunderatz	thunderdocs	247
trainenergyserver_project	trainenergyserver	247
travel_blahg_project	travel_blahg	248
trilium_project	trilium	248
typeorm	typeorm	249
ublock_origin_project	ublock_origin	249
ultrajson_project	ultrajson	250
umbral_project	umbral	251
varktech	pricing_deals_for_woocommerce	252
Vicidial	vicidial	252
videoserver_project	videoserver	254
VIM	vim	255
visser	woocommerce_-_product_importer	258
Vmware	vrealize_log_insight	258

Vendor	Product	Page Number
vprj_project	vprj	259
webswing	webswing	259
windmill_project	windmill	264
withknown	known	264
wormnest_project	wormnest	265
wp-championship_project	wp-championship	265
wp-eventmanager	wp_event_manager	266
wpdevart	gallery	266
wpexperts	wp_contact_slider	267
wp_opt-in_project	wp_opt-in	267
xgenecloud	nocodb	268
Xmlsoft	libxml2	268
xtomo	robo-tom	269
ytdl-sync_project	ytdl-sync	270
Zabbix	Zabbix	270
Zimbra	collaboration	272
Zohocorp	manageengine_adselfservice_plus	273
	manageengine_servicedesk_plus_msp	273
zoo_management_system_project	zoo_management_system	274
Hardware		
amperecomputing	ampere_altra	274
	ampere_altra_max	275
Asus	dsl-n14u-b1	275
gallagher	controller_6000	279
H3C	magic_r100	280
hpe	flexfabric_5945	280
	flexnetwork_5130_ei	280
Kddi	home_spot_cube_2	281
mediatek	mt2601	282
	mt2731	282
	mt2735	283
	mt6297	284

Vendor	Product	Page Number
mediatek	mt6580	285
	mt6725	288
	mt6735	289
	mt6737	292
	mt6739	295
	mt6750	300
	mt6750s	301
	mt6753	303
	mt6755	304
	mt6755s	306
	mt6757	306
	mt6757p	307
	mt6758	308
	mt6761	309
	mt6762	317
	mt6762d	320
	mt6762m	321
	mt6763	322
	mt6765	324
	mt6765t	330
	mt6767	331
	mt6768	332
	mt6769	338
	mt6769t	341
	mt6769z	342
	mt6771	343
	mt6775	349
	mt6779	350
	mt6781	358
	mt6783	366
	mt6785	367
	mt6785t	372

Vendor	Product	Page Number
mediatek	mt6789	373
	mt6795	377
	mt6797	379
	mt6799	381
	mt6833	384
	mt6853	393
	mt6853t	402
	mt6855	404
	mt6873	405
	mt6875	413
	mt6877	417
	mt6879	427
	mt6880	436
	mt6883	438
	mt6885	445
	mt6889	454
	mt6890	461
	mt6891	464
	mt6893	467
	mt6895	476
	mt6983	485
	mt6985	494
	mt8163	495
	mt8167	495
	mt8167s	497
	mt8168	501
	mt8173	505
	mt8175	507
	mt8183	511
	mt8185	515
	mt8321	519
	mt8362a	522

Vendor	Product	Page Number
mediatek	mt8365	527
	mt8385	532
	mt8666	536
	mt8667	541
	mt8675	547
	mt8695	554
	mt8696	554
	mt8735a	557
	mt8735b	558
	mt8765	559
	mt8766	563
	mt8768	570
	mt8771	577
	mt8781	578
	mt8785	579
	mt8786	580
	mt8788	587
	mt8789	594
	mt8791	601
	mt8797	609
	mt8798	617
Nvidia	dgx_a100	619
Omron	na5-12w	622
	na5-15w	624
	na5-7w	625
	na5-9w	627
	nj-pa3001	629
	nj-pd3001	631
	nj101-1000	634
	nj101-1020	636
	nj101-9000	638
	nj101-9020	641

Vendor	Product	Page Number
Omron	nj301-1100	643
	nj301-1200	646
	nj501-1300	648
	nj501-1320	650
	nj501-1340	653
	nj501-140	655
	nj501-1420	658
	nj501-1500	660
	nj501-1520	662
	nj501-4300	665
	nj501-4310	667
	nj501-4320	670
	nj501-4400	672
	nj501-4500	674
	nj501-5300	677
	nj501-r300	679
	nj501-r320	682
	nj501-r400	684
	nj501-r420	686
	nj501-r500	689
	nj501-r520	691
	nx102-1000	694
	nx102-1020	696
	nx102-1100	698
	nx102-1120	701
	nx102-1200	703
	nx102-1220	706
	nx102-9020	708
	nx1p2-1040dt	710
	nx1p2-1040dt1	713
	nx1p2-1140dt	715
	nx1p2-1140dt1	718

Vendor	Product	Page Number
Omron	nx1p2-9024dt	720
	nx1p2-9024dt1	722
	nx1w-adb21	725
	nx1w-cif01	727
	nx1w-cif11	730
	nx1w-cif12	732
	nx1w-dab21v	734
	nx1w-mab221	737
	nx701-1600	739
	nx701-1620	742
	nx701-1700	744
	nx701-1720	746
	nx701-z600	749
	nx701-z700	751
Samsung	exynos_9820	754
Siemens	scalance_x200-4p_irt	754
	scalance_x201-3p_irt	761
	scalance_x201-3p_irt_pro	767
	scalance_x202-2irt	774
	scalance_x202-2p_irt	780
	scalance_x202-2p_irt_pro	787
	scalance_x204-2	794
	scalance_x204-2fm	800
	scalance_x204-2ld	807
	scalance_x204-2ld_ts	813
	scalance_x204-2ts	820
	scalance_x204irt	827
	scalance_x204irt_pro	833
	scalance_x206-1	840
	scalance_x206-1ld	846
	scalance_x208	853
	scalance_x208_pro	860

Vendor	Product	Page Number
Siemens	scalance_x212-2	866
	scalance_x212-2ld	873
	scalance_x216	879
	scalance_x224	886
	scalance_xf201-3p_irt	893
	scalance_xf202-2p_irt	899
	scalance_xf204	906
	scalance_xf204-2	912
	scalance_xf204-2ba_irt	919
	scalance_xf204irt	926
	scalance_xf206-1	932
	scalance_xf208	939
	simatic_cp_1242-7_v2	945
	simatic_cp_1243-1	949
	simatic_cp_1243-7_lte_eu	952
	simatic_cp_1243-7_lte_us	956
	simatic_cp_1243-8_irc	960
	simatic_cp_1542sp-1_irc	963
	simatic_cp_1543-1	967
	simatic_cp_1543sp-1	970
	simatic_mv540_h	974
	simatic_mv540_s	975
	simatic_mv550_h	976
	simatic_mv550_s	978
	simatic_mv560_u	979
	simatic_mv560_x	980
	siplus_et_200sp_cp_1542sp-1_irc_tx_rail	982
	siplus_et_200sp_cp_1543sp-1_isec	985
	siplus_et_200sp_cp_1543sp-1_isec_tx_rail	989
	siplus_net_cp_1242-7_v2	992
	siplus_net_cp_1543-1	996

Vendor	Product	Page Number
Siemens	siplus_s7-1200_cp_1243-1	999
	siplus_s7-1200_cp_1243-1_rail	1003
Tenda	ac10	1006
	ax1803	1007
	ax1806	1007
	m3	1008
Tendacn	ac23_ac2100	1010
totolink	a3000ru	1011
	a3100r	1012
	a800r	1012
	a810r	1013
	a830r	1014
	a950rg	1014
	ex300_v2	1015
	t6	1015
wavlink	wl-wn575a3	1018
webhmi	webhmi	1018
Yokogawa	aw810d	1019
Operating System		
amperecomputing	ampere_altra_firmware	1019
	ampere_altra_max_firmware	1020
Apple	macos	1020
Asus	dsl-n14u-b1_firmware	1020
Debian	debian_linux	1024
Fedoraproject	fedora	1025
gallagher	controller_6000_firmware	1029
Google	android	1031
H3C	magic_r100_firmware	1078
hpe	flexfabric_5945_firmware	1078
	flexnetwork_5130_ei_firmware	1079
IBM	aix	1079
Kddi	home_spot_cube_2_firmware	1080

Vendor	Product	Page Number
Linux	linux_kernel	1080
mediatek	lr11	1088
	lr12	1089
	lr12a	1090
	lr13	1091
	lr9	1092
	nr15	1093
	nr16	1094
Microsoft	windows	1095
	windows_10	1096
	windows_11	1116
	windows_7	1120
	windows_8.1	1122
	windows_rt_8.1	1126
	windows_server_2008	1128
	windows_server_2012	1135
	windows_server_2016	1142
	windows_server_2019	1149
	windows_server_2022	1153
Nvidia	dgx_a100_firmware	1157
Omron	na5-12w_firmware	1160
	na5-15w_firmware	1162
	na5-7w_firmware	1164
	na5-9w_firmware	1165
	nj-pa3001_firmware	1167
	nj-pd3001_firmware	1170
	nj101-1000_firmware	1172
	nj101-1020_firmware	1174
	nj101-9000_firmware	1177
	nj101-9020_firmware	1179
	nj301-1100_firmware	1181
	nj301-1200_firmware	1184

Vendor	Product	Page Number
Omron	nj501-1300_firmware	1186
	nj501-1320_firmware	1189
	nj501-1340_firmware	1191
	nj501-140_firmware	1193
	nj501-1420_firmware	1196
	nj501-1500_firmware	1198
	nj501-1520_firmware	1201
	nj501-4300_firmware	1203
	nj501-4310_firmware	1205
	nj501-4320_firmware	1208
	nj501-4400_firmware	1210
	nj501-4500_firmware	1213
	nj501-5300_firmware	1215
	nj501-r300_firmware	1217
	nj501-r320_firmware	1220
	nj501-r400_firmware	1222
	nj501-r420_firmware	1225
	nj501-r500_firmware	1227
	nj501-r520_firmware	1229
	nx102-1000_firmware	1232
	nx102-1020_firmware	1234
	nx102-1100_firmware	1237
	nx102-1120_firmware	1239
	nx102-1200_firmware	1241
	nx102-1220_firmware	1244
	nx102-9020_firmware	1246
	nx1p2-1040dt1_firmware	1249
	nx1p2-1040dt_firmware	1251
	nx1p2-1140dt1_firmware	1253
	nx1p2-1140dt_firmware	1256
	nx1p2-9024dt1_firmware	1258
	nx1p2-9024dt_firmware	1261

Vendor	Product	Page Number
Omron	nx1w-adb21_firmware	1263
	nx1w-cif01_firmware	1265
	nx1w-cif11_firmware	1268
	nx1w-cif12_firmware	1270
	nx1w-dab21v_firmware	1273
	nx1w-mab221_firmware	1275
	nx701-1600_firmware	1277
	nx701-1620_firmware	1280
	nx701-1700_firmware	1282
	nx701-1720_firmware	1285
	nx701-z600_firmware	1287
	nx701-z700_firmware	1289
Siemens	scalance_x200-4p_irt_firmware	1292
	scalance_x201-3p_irt_firmware	1298
	scalance_x201-3p_irt_pro_firmware	1305
	scalance_x202-2irt_firmware	1312
	scalance_x202-2p_irt_firmware	1318
	scalance_x202-2p_irt_pro_firmware	1325
	scalance_x204-2fm_firmware	1331
	scalance_x204-2ld_firmware	1338
	scalance_x204-2ld_ts_firmware	1345
	scalance_x204-2ts_firmware	1351
	scalance_x204-2_firmware	1358
	scalance_x204irt_firmware	1364
	scalance_x204irt_pro_firmware	1371
	scalance_x206-1ld_firmware	1378
	scalance_x206-1_firmware	1384
	scalance_x208_firmware	1391
	scalance_x208_pro_firmware	1397
	scalance_x212-2ld_firmware	1404
	scalance_x212-2_firmware	1411
	scalance_x216_firmware	1417

Vendor	Product	Page Number
Siemens	scalance_x224_firmware	1424
	scalance_xf201-3p_irt_firmware	1430
	scalance_xf202-2p_irt_firmware	1437
	scalance_xf204-2ba_irt_firmware	1444
	scalance_xf204-2_firmware	1450
	scalance_xf204irt_firmware	1457
	scalance_xf204_firmware	1463
	scalance_xf206-1_firmware	1470
	scalance_xf208_firmware	1477
	simatic_cp_1242-7_v2_firmware	1483
	simatic_cp_1243-1_firmware	1487
	simatic_cp_1243-7_lte_eu_firmware	1490
	simatic_cp_1243-7_lte_us_firmware	1494
	simatic_cp_1243-8_irc_firmware	1497
	simatic_cp_1542sp-1_irc_firmware	1501
	simatic_cp_1543-1_firmware	1504
	simatic_cp_1543sp-1_firmware	1508
	simatic_mv540_h_firmware	1512
	simatic_mv540_s_firmware	1513
	simatic_mv550_h_firmware	1514
	simatic_mv550_s_firmware	1515
	simatic_mv560_u_firmware	1517
	simatic_mv560_x_firmware	1518
	siplus_et_200sp_cp_1542sp-1_irc_tx_rail_firmware	1519
	siplus_et_200sp_cp_1543sp-1_isec_firmware	1523
	siplus_et_200sp_cp_1543sp-1_isec_tx_rail_firmware	1526
	siplus_net_cp_1242-7_v2_firmware	1530
	siplus_net_cp_1543-1_firmware	1533
	siplus_s7-1200_cp_1243-1_firmware	1537

Vendor	Product	Page Number
Siemens	siplus_s7-1200_cp_1243-1_rail_firmware	1541
Tenda	ac10_firmware	1544
	ax1803_firmware	1544
	ax1806_firmware	1545
	m3_firmware	1546
Tendacn	ac23_ac2100_firmware	1547
totolink	a3000ru_firmware	1549
	a3100r_firmware	1550
	a800r_firmware	1550
	a810r_firmware	1551
	a830r_firmware	1551
	a950rg_firmware	1552
	ex300_v2_firmware	1552
	t6_firmware	1553
wavlink	wl-wn575a3_firmware	1555
webhmi	webhmi_firmware	1556
XEN	xen	1556
Yokogawa	aw810d_firmware	1560

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: aceattorneyonline					
Product: akashi					
Affected Version(s): * Up to (excluding) 1.4					
Improper Validation of Array Index	07-Jul-2022	7.5	Akashi is an open source server implementation of the Attorney Online video game based on the Ace Attorney universe. Affected versions of Akashi are subject to a denial of service attack. An attacker can use a specially crafted evidence packet to make an illegal modification, causing a server crash. This can be used to mount a denial-of-service exploit. Users are advised to upgrade. There is no known workaround for this issue. **CVE ID : CVE-2022-31135**	https://github.com/AttorneyOnline/akashi/security/advisories/GHSA-vj86-vfmg-q68v, https://github.com/AttorneyOnline/akashi/commit/5566cdfedddef1f219aee33477d9c9690bf2f78b	A-ACE-AKAS-200722/1
Vendor: adminite					
Product: adminlte					
Affected Version(s): * Up to (excluding) 5.13					
Improper Neutralization of Input During Web Page Generation	07-Jul-2022	4.8	AdminLTE is a Pi-hole Dashboard for stats and configuration. In affected versions inserting code like `<script>alert("XSS")</script>` in the field	https://github.com/pi-hole/AdminLTE/security/advisories/GHSA-cfr5-rqm5-9vhp,	A-ADM-ADMI-200722/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			marked with "Domain to look for" and hitting <kbd>enter</kbd> (or clicking on any of the buttons) will execute the script. The user must be logged in to use this vulnerability. Usually only administrators have login access to pi-hole, minimizing the risks. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-31029**	https://github.com/pi-hole/AdminLTE/commit/b07372bd426ca8111824a0244dc89d07a7243509	
Vendor: admin_management_xtended_project					
Product: admin_management_xtended					
Affected Version(s): * Up to (excluding) 2.4.5					
Cross-Site Request Forgery (CSRF)	11-Jul-2022	6.5	The Admin Management Xtended WordPress plugin before 2.4.5 does not have CSRF checks in some of its AJAX actions, allowing attackers to make a logged users with the right capabilities to call them. This can lead to changes in post status (draft, published), slug, post date, comment status (enabled, disabled) and more. **CVE ID : CVE-2022-1599**	N/A	A-ADM-ADMI-200722/3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: agilepoint					
Product: agilepoint_nx					
Affected Version(s): * Up to (excluding) 8.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jul-2022	8.8	Editable SQL Queries behind Base64 encoding sending from the Client-Side to The Server-Side for a particular API used in legacy Work Center module. He attack is available for any authenticated user, in any kind of rule. under the function : /AgilePointServer/Extension/FetchUsingEncodedData in the parameter: EncodedData **CVE ID : CVE-2022-30619**	N/A	A-AGI-AGIL-200722/4
Vendor: anuvaad-corpus_project					
Product: anuvaad-corpus					
Affected Version(s): * Up to (including) 2020-11-23					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The project-anuvaad/anuvaad-corpus repository through 2020-11-23 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31552**	N/A	A-ANU-ANUV-200722/5
Vendor: Apache					
Product: commons_configuration					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2.4 Up to (excluding) 2.8					
N/A	06-Jul-2022	9.8	Apache Commons Configuration performs variable interpolation, allowing properties to be dynamically evaluated and expanded. The standard format for interpolation is "${prefix:name}", where "prefix" is used to locate an instance of org.apache.commons.configuration2.interpol.Lookup that performs the interpolation. Starting with version 2.4 and continuing through 2.7, the set of default Lookup instances included interpolators that could result in arbitrary code execution or contact with remote servers. These lookups are: - "script" - execute expressions using the JVM script execution engine (javax.script) - "dns" - resolve dns records - "url" - load values from urls, including from remote servers Applications using the interpolation defaults in the affected versions may be	https://lists.apache.org/thread/tdf5n7j80lfxdhs2764vn0xmpfodm87s	A-APA-COMM-200722/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to remote code execution or unintentional contact with remote servers if untrusted configuration values are used. Users are recommended to upgrade to Apache Commons Configuration 2.8.0, which disables the problematic interpolators by default. **CVE ID : CVE-2022-33980**		
Product: druid					
Affected Version(s): * Up to (excluding) 0.23.0					
Improper Restriction of Rendered UI Layers or Frames	07-Jul-2022	4.3	In Apache Druid 0.22.1 and earlier, the server did not set appropriate headers to prevent clickjacking. Druid 0.23.0 and later prevent clickjacking using the Content-Security-Policy header. **CVE ID : CVE-2022-28889**	https://lists.apache.org/thread/t3nsq4crdr8wqgmj721d2wg6pf26s5cw	A-APA-DRUI-200722/7
Vendor: appfire					
Product: jira_misc_custom_fields					
Affected Version(s): 2.4.6					
Improper Neutralization of Input During Web Page	07-Jul-2022	5.4	The Appfire Jira Misc Custom Fields (JMCF) app 2.4.6 for Atlassian Jira allows XSS via a crafted project name to the Add Auto	N/A	A-APP-JIRA-200722/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Indexing Rule function. **CVE ID : CVE-2022-32567**		
Vendor: audio_aligner_app_project					
Product: audio_aligner_app					
Affected Version(s): * Up to (including) 2020-01-10					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The longmaoteamtf/audio_aligner_app repository through 2020-01-10 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31577**	N/A	A-AUD-AUDI-200722/9
Vendor: automatedquizeval_project					
Product: automatedquizeval					
Affected Version(s): * Up to (including) 2020-04-27					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The sravaniboinepelli/AutomatedQuizEval repository through 2020-04-27 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31583**	N/A	A-AUT-AUTO-200722/10
Vendor: automox					
Product: automox					
Affected Version(s): * Up to (excluding) 37					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	01-Jul-2022	7	The Automox Agent installation package before 37 on macOS allows an unprivileged user to obtain root access because of incorrect access control on a file used within the PostInstall script. **CVE ID : CVE-2022-27904**	https://automox.com, https://www.automox.com/security/security-bulletin	A-AUT-AUTO-200722/11
Vendor: averta					
Product: shortcodes_and_extra_features_for_phlox_theme					
Affected Version(s): * Up to (excluding) 2.9.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2022	6.1	The Shortcodes and extra features for Phlox WordPress plugin before 2.9.8 does not sanitise and escape a parameter before outputting it back in the response, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-1910**	N/A	A-AVE-SHOR-200722/12
Vendor: awin					
Product: awin_data_feed					
Affected Version(s): * Up to (including) 1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2022	6.1	The Awin Data Feed WordPress plugin through 1.6 does not sanitise and escape a parameter before outputting it back via an AJAX action (available to both unauthenticated and authenticated users),	N/A	A-AWI-AWIN-200722/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-1937**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2022	5.4	The Awin Data Feed WordPress plugin through 1.6 does not sanitise and escape a header when processing request to generate analytics data, allowing unauthenticated users to perform Stored Cross-Site Scripting attacks against a logged in admin viewing the plugin's settings **CVE ID : CVE-2022-1938**	N/A	A-AWI-AWIN-200722/14
Vendor: baiduwenkuspider_flaskweb_project					
Product: baiduwenkuspider_flaskweb					
Affected Version(s): * Up to (excluding) 2021-11-29					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The ChangeWeDer/BaiduWenkuSpider_flaskWeb repository before 2021-11-29 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31504**	https://github.com/ChangeWeDer/BaiduWenkuSpider_flaskWeb/pull/3	A-BAI-BAID-200722/15
Vendor: barry_voice_assistant_project					
Product: barry_voice_assistant					
Affected Version(s): * Up to (including) 2021-01-18					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The lyubolp/Barry-Voice-Assistant repository through 2021-01-18 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31541**	N/A	A-BAR-BARR-200722/16
Vendor: beego					
Product: beego					
Affected Version(s): * Up to (including) 2.0.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2022	9.8	The leafInfo.match() function in Beego v2.0.3 and below uses path.join() to deal with wildcardvalues which can lead to cross directory risk. **CVE ID : CVE-2022-31836**	https://github.com/beego/beego/issues/4961	A-BEE-BEEG-200722/17
Vendor: bold-themes					
Product: bold_page_builder					
Affected Version(s): * Up to (excluding) 4.3.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2022	4.8	The Bold Page Builder WordPress plugin before 4.3.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed.	N/A	A-BOL-BOLD-200722/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2089		
Vendor: bonn_activity_maps_annotation_tool_project					
Product: bonn_activity_maps_annotation_tool					
Affected Version(s): * Up to (including) 2021-08-31					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The bonn-activity-maps/bam_annotation_tool repository through 2021-08-31 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31528**	N/A	A-BON-BONN-200722/19
Vendor: bt_lnmp_project					
Product: bt_lnmp					
Affected Version(s): * Up to (including) 2019-10-10					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	7.5	The piaoyunsoft/bt_lnmp repository through 2019-10-10 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31578**	N/A	A-BT_-BT_L-200722/20
Vendor: carceresbe_project					
Product: carceresbe					
Affected Version(s): 1.0					
Improper Limitation of a Pathname	11-Jul-2022	9.3	The Delor4/CarceresBE repository through 1.0 on GitHub allows	N/A	A-CAR-CARC-200722/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31515**		
Vendor: caretakerr-api_project					
Product: caretakerr-api					
Affected Version(s): * Up to (including) 2021-05-17					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The sanojtharindu/caretakerr-api repository through 2021-05-17 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31580**	N/A	A-CAR-CARE-200722/22
Vendor: ceneo-web-scrapper_project					
Product: ceneo-web-scrapper					
Affected Version(s): * Up to (including) 2021-03-15					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.8	The adriankoczuruek/ceneo-web-scrapper repository through 2021-03-15 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31570**	N/A	A-CEN-CENE-200722/23
Vendor: chafa_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: chafa					
Affected Version(s): * Up to (excluding) 1.10.3					
Out-of-bounds Read	04-Jul-2022	5.5	Buffer Over-read in GitHub repository hpjansson/chafa prior to 1.10.3. **CVE ID : CVE-2022-2301**	https://github.com/hpjansson/chafa/commit/56fabfa18a6880b4cb66047fa655792007804 8d9, https://huntr.dev/bounties/f6b9114b-671d-4948-b946-ffe5c9aeb816	A-CHA-CHAF-200722/24
Vendor: chainer					
Product: chainerrl-visualizer					
Affected Version(s): * Up to (including) 0.1.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The chainer/chainerrl-visualizer repository through 0.1.1 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31573**	N/A	A-CHA-CHAI-200722/25
Vendor: changepop-back_project					
Product: changepop-back					
Affected Version(s): * Up to (including) 2019-06-04					
Improper Limitation of a Pathname to a Restricted Directory	11-Jul-2022	9.3	The unizar-30226-2019-06/ChangePop-Back repository through 2019-06-04 on GitHub allows absolute path traversal because the	N/A	A-CHA-CHAN-200722/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			Flask send_file function is used unsafely. **CVE ID : CVE-2022-31586**		
Vendor: Checkpoint					
Product: endpoint_security					
Affected Version(s): e83					
N/A	07-Jul-2022	2.3	Check Point Endpoint before version E86.50 failed to protect against specific registry change which allowed to disable endpoint protection by a local administrator. **CVE ID : CVE-2022-23744**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk179609	A-CHE-ENDP-200722/27
Affected Version(s): e84					
N/A	07-Jul-2022	2.3	Check Point Endpoint before version E86.50 failed to protect against specific registry change which allowed to disable endpoint protection by a local administrator. **CVE ID : CVE-2022-23744**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk179609	A-CHE-ENDP-200722/28
Affected Version(s): e85					
N/A	07-Jul-2022	2.3	Check Point Endpoint before version E86.50 failed to protect against specific registry change which allowed to disable endpoint protection	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&s	A-CHE-ENDP-200722/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by a local administrator. **CVE ID : CVE-2022-23744**	olutionid=sk179609	
Affected Version(s): e86.10					
N/A	07-Jul-2022	2.3	Check Point Endpoint before version E86.50 failed to protect against specific registry change which allowed to disable endpoint protection by a local administrator. **CVE ID : CVE-2022-23744**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk179609	A-CHE-ENDP-200722/30
Affected Version(s): e86.20					
N/A	07-Jul-2022	2.3	Check Point Endpoint before version E86.50 failed to protect against specific registry change which allowed to disable endpoint protection by a local administrator. **CVE ID : CVE-2022-23744**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk179609	A-CHE-ENDP-200722/31
Affected Version(s): e86.30					
N/A	07-Jul-2022	2.3	Check Point Endpoint before version E86.50 failed to protect against specific registry change which allowed to disable endpoint protection by a local administrator. **CVE ID : CVE-2022-23744**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk179609	A-CHE-ENDP-200722/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): e86.40					
N/A	07-Jul-2022	2.3	Check Point Endpoint before version E86.50 failed to protect against specific registry change which allowed to disable endpoint protection by a local administrator. **CVE ID : CVE-2022-23744**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk179609	A-CHE-ENDP-200722/33
Product: harmony_endpoint					
Affected Version(s): e83					
N/A	07-Jul-2022	2.3	Check Point Endpoint before version E86.50 failed to protect against specific registry change which allowed to disable endpoint protection by a local administrator. **CVE ID : CVE-2022-23744**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk179609	A-CHE-HARM-200722/34
Affected Version(s): e84					
N/A	07-Jul-2022	2.3	Check Point Endpoint before version E86.50 failed to protect against specific registry change which allowed to disable endpoint protection by a local administrator. **CVE ID : CVE-2022-23744**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk179609	A-CHE-HARM-200722/35
Affected Version(s): e85					
N/A	07-Jul-2022	2.3	Check Point Endpoint before version E86.50	https://supportcenter.checkp	A-CHE-HARM-200722/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failed to protect against specific registry change which allowed to disable endpoint protection by a local administrator. **CVE ID : CVE-2022-23744**	oint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk179609	
Affected Version(s): e86.10					
N/A	07-Jul-2022	2.3	Check Point Endpoint before version E86.50 failed to protect against specific registry change which allowed to disable endpoint protection by a local administrator. **CVE ID : CVE-2022-23744**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk179609	A-CHE-HARM-200722/37
Affected Version(s): e86.20					
N/A	07-Jul-2022	2.3	Check Point Endpoint before version E86.50 failed to protect against specific registry change which allowed to disable endpoint protection by a local administrator. **CVE ID : CVE-2022-23744**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk179609	A-CHE-HARM-200722/38
Affected Version(s): e86.30					
N/A	07-Jul-2022	2.3	Check Point Endpoint before version E86.50 failed to protect against specific registry change which allowed to disable endpoint protection	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&s	A-CHE-HARM-200722/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by a local administrator. **CVE ID : CVE-2022-23744**	olutionid=sk179609	
Affected Version(s): e86.40					
N/A	07-Jul-2022	2.3	Check Point Endpoint before version E86.50 failed to protect against specific registry change which allowed to disable endpoint protection by a local administrator. **CVE ID : CVE-2022-23744**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk179609	A-CHE-HARM-200722/40
Vendor: Cisco					
Product: expressway					
Affected Version(s): * Up to (excluding) x14.0.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2022	6.5	Multiple vulnerabilities in the API and in the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow a remote attacker to overwrite arbitrary files or conduct null byte poisoning attacks on an affected device. Note: Cisco Expressway Series refers to the Expressway Control (Expressway-C) device and the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-overwrite-3buqW8LH	A-CIS-EXPR-200722/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Expressway Edge (Expressway-E) device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20812**		
Improper Certificate Validation	06-Jul-2022	5.9	Multiple vulnerabilities in the API and in the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow a remote attacker to overwrite arbitrary files or conduct null byte poisoning attacks on an affected device. Note: Cisco Expressway Series refers to the Expressway Control (Expressway-C) device and the Expressway Edge (Expressway-E) device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20813**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-overwrite-3buqW8LH	A-CIS-EXPR-200722/42
Product: smart_software_manager_on-prem					
Affected Version(s): From (including) 8 Up to (excluding) 8-202112					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	06-Jul-2022	6.5	A vulnerability in Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to incorrect handling of multiple simultaneous device registrations on Cisco SSM On-Prem. An attacker could exploit this vulnerability by sending multiple device registration requests to Cisco SSM On-Prem. A successful exploit could allow the attacker to cause a DoS condition on an affected device. **CVE ID : CVE-2022-20808**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-privesc-tP6uNZOS	A-CIS-SMAR-200722/43
Product: telepresence_collaboration_endpoint					
Affected Version(s): * Up to (excluding) 10.15.2.2					
Insertion of Sensitive Information into Log File	06-Jul-2022	4.9	A vulnerability in the logging component of Cisco TelePresence Collaboration Endpoint (CE) and RoomOS Software could allow an authenticated, remote attacker to view sensitive information in clear text on an affected system. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-infodisc-YOTz9Ct7	A-CIS-TELE-200722/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the storage of certain unencrypted credentials. An attacker could exploit this vulnerability by accessing the audit logs on an affected system and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to use those credentials to access confidential information, some of which may contain personally identifiable information (PII). Note: To access the logs that are stored in the RoomOS Cloud, an attacker would need valid Administrator-level credentials. **CVE ID : CVE-2022-20768**		
Product: telepresence_video_communication_server					
Affected Version(s): * Up to (excluding) x14.0.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2022	6.5	Multiple vulnerabilities in the API and in the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow a remote attacker to overwrite	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-overwrite-3buqW8LH	A-CIS-TELE-200722/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary files or conduct null byte poisoning attacks on an affected device. Note: Cisco Expressway Series refers to the Expressway Control (Expressway-C) device and the Expressway Edge (Expressway-E) device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20812**		
Improper Certificate Validation	06-Jul-2022	5.9	Multiple vulnerabilities in the API and in the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow a remote attacker to overwrite arbitrary files or conduct null byte poisoning attacks on an affected device. Note: Cisco Expressway Series refers to the Expressway Control (Expressway-C) device and the Expressway Edge (Expressway-E)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-overwrite-3buqW8LH	A-CIS-TELE-200722/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20813**		
Product: unified_communications_manager					
Affected Version(s): * Up to (excluding) 12.5\\(1\\)su6					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2022	4.3	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to read arbitrary files on the underlying operating system of an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to access	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-file-read-qgjhEc3A	A-CIS-UNIF-200722/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive files on the operating system. **CVE ID : CVE-2022-20862**		
Affected Version(s): * Up to (including) 11.5\\(1.10000.6\\)					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2022	6.5	A vulnerability in the database user privileges of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an authenticated, remote attacker to read arbitrary files on the underlying operating system of an affected device. This vulnerability is due to insufficient file permission restrictions. An attacker could exploit this vulnerability by sending a crafted command from the API to the application. A successful exploit could allow the attacker to read arbitrary files on the underlying operating	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-imp-afr-YBFLNyzd	A-CIS-UNIF-200722/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system of the affected device. The attacker would need valid user credentials to exploit this vulnerability. **CVE ID : CVE-2022-20791**		
Affected Version(s): From (including) 11.5\\(1\\) Up to (excluding) 14su2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2022	6.1	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-RgH7MpKA	A-CIS-UNIF-200722/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2022-20800**		
Affected Version(s): From (including) 12.5 Up to (including) 12.5\\(1.10000.22\\)					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2022	6.5	A vulnerability in the database user privileges of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an authenticated, remote attacker to read arbitrary files on the underlying operating system of an affected device. This vulnerability is due to insufficient file permission restrictions. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-imp-afr-YBFLNyzd	A-CIS-UNIF-200722/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending a crafted command from the API to the application. A successful exploit could allow the attacker to read arbitrary files on the underlying operating system of the affected device. The attacker would need valid user credentials to exploit this vulnerability. **CVE ID : CVE-2022-20791**		
Affected Version(s): From (including) 12.5\\(1\\) Up to (excluding) 12.5\\(1\\)su6					
Observable Discrepancy	06-Jul-2022	5.3	A vulnerability in Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to perform a timing attack. This vulnerability is due to insufficient protection of a system password. An attacker could exploit this vulnerability by observing the time it takes the system to respond to various	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-timing-JVbHECOK	A-CIS-UNIF-200722/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			queries. A successful exploit could allow the attacker to determine a sensitive system password. **CVE ID : CVE-2022-20752**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14su1					
Observable Discrepancy	06-Jul-2022	5.3	A vulnerability in Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to perform a timing attack. This vulnerability is due to insufficient protection of a system password. An attacker could exploit this vulnerability by observing the time it takes the system to respond to various queries. A successful exploit could allow the attacker to determine a sensitive system password. **CVE ID : CVE-2022-20752**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-timing-JVbHECOK	A-CIS-UNIF-200722/52
Affected Version(s): From (including) 14.0 Up to (excluding) 14su2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jul-2022	8.8	A vulnerability in the Disaster Recovery framework of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), and Cisco Unity Connection could allow an authenticated, remote attacker to perform certain administrative actions they should not be able to. This vulnerability is due to insufficient access control checks on the affected device. An attacker with read-only privileges could exploit this vulnerability by executing a specific vulnerable command on an affected device. A successful exploit could allow the attacker to perform a set of administrative actions they should not be able to. **CVE ID : CVE-2022-20859**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-access-dMKvV2DY	A-CIS-UNIF-200722/53
Improper Neutralization of Input During	06-Jul-2022	6.1	A vulnerability in the web-based management interface of Cisco Unified	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis	A-CIS-UNIF-200722/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Communications Manager (Unified CM), Cisco Unified CM Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2022-20815**	co-sa-cucm-xss-ksKd5yfA	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2022	4.3	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to read arbitrary files on the underlying operating system of an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to access sensitive files on the operating system. **CVE ID : CVE-2022-20862**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-file-read-qgjhEc3A	A-CIS-UNIF-200722/55
Affected Version(s): From (including) 14.0 Up to (including) 14.0\\(1.10000.20\\)					
Improper Limitation of a Pathname	06-Jul-2022	6.5	A vulnerability in the database user privileges of Cisco Unified	https://tools.cisco.com/security/center/content/CiscoSecur	A-CIS-UNIF-200722/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an authenticated, remote attacker to read arbitrary files on the underlying operating system of an affected device. This vulnerability is due to insufficient file permission restrictions. An attacker could exploit this vulnerability by sending a crafted command from the API to the application. A successful exploit could allow the attacker to read arbitrary files on the underlying operating system of the affected device. The attacker would need valid user credentials to exploit this vulnerability. **CVE ID : CVE-2022-20791**	ityAdvisory/cisco-sa-cucm-imp-afr-YBFLNyzd	
Product: unified_communications_manager_im_and_presence_service					
Affected Version(s): From (including) 12.5\\(1\\) Up to (excluding) 12.5\\(1\\)su6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2022	6.1	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified CM Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-ksKd5yfA	A-CIS-UNIF-200722/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			browser-based information. **CVE ID : CVE-2022-20815**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14su2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2022	6.5	A vulnerability in the database user privileges of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an authenticated, remote attacker to read arbitrary files on the underlying operating system of an affected device. This vulnerability is due to insufficient file permission restrictions. An attacker could exploit this vulnerability by sending a crafted command from the API to the application. A successful exploit could allow the attacker to read arbitrary files on the underlying operating	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-imp-afr-YBFLNyzd	A-CIS-UNIF-200722/58

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system of the affected device. The attacker would need valid user credentials to exploit this vulnerability. **CVE ID : CVE-2022-20791**		
Affected Version(s): * Up to (including) 12.5\\(1\\)					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2022	6.5	A vulnerability in the database user privileges of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an authenticated, remote attacker to read arbitrary files on the underlying operating system of an affected device. This vulnerability is due to insufficient file permission restrictions. An attacker could exploit this vulnerability by sending a crafted command from the API to the application. A successful exploit could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-imp-afr-YBFLNyzd	A-CIS-UNIF-200722/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to read arbitrary files on the underlying operating system of the affected device. The attacker would need valid user credentials to exploit this vulnerability. **CVE ID : CVE-2022-20791**		
Affected Version(s): From (including) 11.5\\(1\\) Up to (excluding) 11.5\\(1\\)su11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2022	6.1	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified CM Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-ksKd5yfA	A-CIS-UNIF-200722/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2022-20815**		
Affected Version(s): From (including) 11.5\\(1\\) Up to (excluding) 12.5\\(1\\)su5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2022	6.1	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-RgH7MpKA	A-CIS-UNIF-200722/61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2022-20800**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14.0su2					
Incorrect Authorization	06-Jul-2022	8.8	A vulnerability in the Disaster Recovery framework of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), and Cisco Unity Connection could allow an authenticated, remote attacker to perform certain administrative actions they should not be able to. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-access-dMKvV2DY	A-CIS-UNIF-200722/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient access control checks on the affected device. An attacker with read-only privileges could exploit this vulnerability by executing a specific vulnerable command on an affected device. A successful exploit could allow the attacker to perform a set of administrative actions they should not be able to. **CVE ID : CVE-2022-20859**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2022	6.1	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified CM Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-ksKd5yfA	A-CIS-UNIF-200722/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2022-20815**		
Product: unity_connection					
Affected Version(s): From (including) 11.5\\(1\\) Up to (excluding) 14su2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2022	6.1	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), and Cisco Unity Connection	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-RgH7MpKA	A-CIS-UNIT-200722/64

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2022-20800**		
Affected Version(s): From (including) 12.5\\(1\\) Up to (excluding) 12.5\\(1\\)su6					
Observable Discrepancy	06-Jul-2022	5.3	A vulnerability in Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-timing-JVbHECOK	A-CIS-UNIT-200722/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to perform a timing attack. This vulnerability is due to insufficient protection of a system password. An attacker could exploit this vulnerability by observing the time it takes the system to respond to various queries. A successful exploit could allow the attacker to determine a sensitive system password. **CVE ID : CVE-2022-20752**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14su1					
Observable Discrepancy	06-Jul-2022	5.3	A vulnerability in Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to perform a timing attack. This vulnerability is due to insufficient protection of a system password. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-timing-JVbHECOK	A-CIS-UNIT-200722/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			observing the time it takes the system to respond to various queries. A successful exploit could allow the attacker to determine a sensitive system password. **CVE ID : CVE-2022-20752**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14su2					
Incorrect Authorization	06-Jul-2022	8.8	A vulnerability in the Disaster Recovery framework of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), and Cisco Unity Connection could allow an authenticated, remote attacker to perform certain administrative actions they should not be able to. This vulnerability is due to insufficient access control checks on the affected device. An attacker with read-only privileges could exploit this vulnerability by executing a specific vulnerable command on an affected device. A successful exploit could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-access-dMKvV2DY	A-CIS-UNIT-200722/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to perform a set of administrative actions they should not be able to. **CVE ID : CVE-2022-20859**		
Vendor: citeum					
Product: opencti					
Affected Version(s): * Up to (including) 5.2.4					
Incorrect Authorization	05-Jul-2022	7.5	In OpenCTI through 5.2.4, a broken access control vulnerability has been identified in the profile endpoint. An attacker can abuse the identified vulnerability in order to arbitrarily change their registered e-mail address as well as their API key, even though such action is not possible through the interface, legitimately. **CVE ID : CVE-2022-30290**	N/A	A-CIT-OPEN-200722/68
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2022	5.4	A stored Cross-site Scripting (XSS) vulnerability was identified in the Data Import functionality of OpenCTI through 5.2.4. An attacker can abuse the vulnerability to upload a malicious file that will then be executed by a victim when they open the file location.	N/A	A-CIT-OPEN-200722/69

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30289		
Vendor: clinic\'s_patient_management_system_project					
Product: clinic\'s_patient_management_system					
Affected Version(s): 2.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Jul-2022	9.8	A vulnerability has been found in SourceCodester Clinics Patient Management System 2.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /pms/index.php of the component Login Page. The manipulation of the argument user_name with the input admin' or '1'='1 leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2022-2298**	N/A	A-CLI-CLIN-200722/70
Unrestricted Upload of File with Dangerous Type	12-Jul-2022	8.8	A vulnerability, which was classified as critical, was found in SourceCodester Clinics Patient Management System 2.0. Affected is an unknown function of the file /pms/update_user.php?user_id=1. The manipulation of the	N/A	A-CLI-CLIN-200722/71

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument profile_picture with the input <?php phpinfo();?> leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2022-2297**		
Vendor: CMU					
Product: opendiamond					
Affected Version(s): * Up to (including) 10.1.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The cmusatyalab/opendiamond repository through 10.1.1 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31506**	https://github.com/cmusatyalab/opendiamond/commit/398049c187ee644beabab44d6fece82251c1ea56	A-CMU-OPEN-200722/72
Vendor: cockybook_project					
Product: cockybook					
Affected Version(s): * Up to (including) 2015-04-16					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The ceee-vip/cockybook repository through 2015-04-16 on GitHub allows absolute path traversal because the Flask send_file	N/A	A-COC-COCK-200722/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function is used unsafely. **CVE ID : CVE-2022-31572**		
Vendor: Codesys					
Product: opc_da_server					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.5.18.20					
Unprotected Storage of Credentials	11-Jul-2022	5.5	The CODESYS OPC DA Server prior V3.5.18.20 stores PLC passwords as plain text in its configuration file so that it is visible to all authorized Microsoft Windows users of the system. **CVE ID : CVE-2022-1794**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17129&token=1c1485c4a700c04f2069699f5be7558d276ca117&download=	A-COD-OPC_-200722/74
Vendor: Codologic					
Product: codoforum					
Affected Version(s): 5.1					
Unrestricted Upload of File with Dangerous Type	07-Jul-2022	7.2	Codoforum v5.1 was discovered to contain an arbitrary file upload vulnerability via the logo change option in the admin panel. **CVE ID : CVE-2022-31854**	https://codoforum.com	A-COD-CODO-200722/75
Vendor: college_management_system_project					
Product: college_management_system					
Affected Version(s): 1.0					
N/A	01-Jul-2022	8.8	College Management System v1.0 was discovered to contain a remote code execution (RCE)	N/A	A-COL-COLL-200722/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability via /College/admin/teacher.php. This vulnerability is exploited via a crafted PHP file. **CVE ID : CVE-2022-32420**		
Vendor: comment_license_project					
Product: comment_license					
Affected Version(s): * Up to (excluding) 1.4.0					
Cross-Site Request Forgery (CSRF)	11-Jul-2022	4.3	The Comment License WordPress plugin before 1.4.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack **CVE ID : CVE-2022-1957**	N/A	A-COM-COMM-200722/77
Vendor: control-webpanel					
Product: webpanel					
Affected Version(s): * Up to (including) 0.9.8.1124					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Jul-2022	9.8	A path traversal vulnerability in loader.php of CWP v0.9.8.1122 allows attackers to execute arbitrary code via a crafted POST request. **CVE ID : CVE-2022-25046**	N/A	A-CON-WEBP-200722/78
Affected Version(s): 0.9.8.1126					
Improper Neutralization of	07-Jul-2022	8.8	Command injection vulnerability in CWP v0.9.8.1126 that	N/A	A-CON-WEBP-200722/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			allows normal users to run commands as the root user. **CVE ID : CVE-2022-25048**		
Use of Insufficiently Random Values	07-Jul-2022	5.9	The password reset token in CWP v0.9.8.1126 is generated using known or predictable values. **CVE ID : CVE-2022-25047**	N/A	A-CON-WEBP-200722/80
Vendor: csm_server_project					
Product: csm_server					
Affected Version(s): * Up to (including) 3.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The csm-aut/csm repository through 3.5 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31530**	N/A	A-CSM-CSM_-200722/81
Vendor: cuyz					
Product: valinor					
Affected Version(s): * Up to (excluding) 0.12.0					
Generation of Error Message Containing Sensitive Information	11-Jul-2022	9.1	Valinor is a PHP library that helps to map any input into a strongly-typed value object structure. Prior to version 0.12.0, Valinor can use `Throwable#getMess	https://github.com/CuyZ/Valinor/security/advisories/GHSA-5pgm-3j3g-2rc7	A-CUY-VALI-200722/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			age()` when it should not have permission to do so. This is a problem with cases such as an SQL exception showing an SQL snippet, a database connection exception showing database IP address/username/password, or a timeout detail / out of memory detail. Attackers could use this information for potential data exfiltration, denial of service attacks, enumeration attacks, etc. Version 0.12.0 contains a patch for this vulnerability. **CVE ID : CVE-2022-31140**		
Vendor: Cybozu					
Product: garoon					
Affected Version(s): From (including) 4.0.0 Up to (including) 5.5.1					
Allocation of Resources Without Limits or Throttling	04-Jul-2022	6.5	Improper input validation vulnerability in Space of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to repeatedly display errors in certain functions and cause a denial-of-service (DoS). **CVE ID : CVE-2022-29892**	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	04-Jul-2022	5.4	Browse restriction bypass and operation restriction bypass vulnerability in Cabinet of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to alter and/or obtain the data of Cabinet. **CVE ID : CVE-2022-26368**	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/84
Incorrect Permission Assignment for Critical Resource	04-Jul-2022	4.3	Operation restriction bypass vulnerability in Portal of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to alter the data of Portal. **CVE ID : CVE-2022-26051**	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/85
Incorrect Permission Assignment for Critical Resource	04-Jul-2022	4.3	Operation restriction bypass vulnerability in Link of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to alter the data of Link. **CVE ID : CVE-2022-26054**	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/86
Incorrect Authorization	04-Jul-2022	4.3	Operation restriction bypass vulnerability in Workflow of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to alter the data of Workflow.	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-27661		
Improper Input Validation	04-Jul-2022	4.3	Improper input validation vulnerability in Space of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to alter the data of Space. **CVE ID : CVE-2022-27803**	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/88
Incorrect Permission Assignment for Critical Resource	04-Jul-2022	4.3	Improper input validation vulnerability in Link of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to disable to add Categories. **CVE ID : CVE-2022-27807**	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/89
Incorrect Permission Assignment for Critical Resource	04-Jul-2022	4.3	Improper input validation vulnerability in Scheduler of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to alter the data of Scheduler. **CVE ID : CVE-2022-28692**	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/90
Incorrect Authorization	04-Jul-2022	4.3	Operation restriction bypass vulnerability in Bulletin of Cybozu Garoon 4.0.0 to 5.5.1 allow a remote authenticated attacker to alter the data of Bulletin.	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28718		
N/A	11-Jul-2022	4.3	Browse restriction bypass vulnerability in Cabinet of Cybozu Garoon 4.0.0 to 5.5.1 allows a remote authenticated attacker to obtain the data of Cabinet. **CVE ID : CVE-2022-31472**	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/92
Affected Version(s): From (including) 4.0.0 Up to (including) 5.9.0					
Incorrect Authorization	04-Jul-2022	8.1	Operation restriction bypass vulnerability in Space of Cybozu Garoon 4.0.0 to 5.9.0 allows a remote authenticated attacker to delete the data of Space. **CVE ID : CVE-2022-29484**	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/93
Affected Version(s): From (including) 4.0.0 Up to (including) 5.9.1					
N/A	11-Jul-2022	8.1	Operation restriction bypass in multiple applications of Cybozu Garoon 4.0.0 to 5.9.1 allows a remote authenticated attacker to alter the file information and/or delete the files. **CVE ID : CVE-2022-30602**	https://cs.cybozu.co.jp/2022/007682.html	A-CYB-GARO-200722/94
Missing Authorization	11-Jul-2022	6.5	Exposure of sensitive information to an unauthorized actor issue in multiple applications of	https://cs.cybozu.co.jp/2022/007682.html	A-CYB-GARO-200722/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cybozu Garoon 4.0.0 to 5.9.1 allows a remote authenticated attacker to obtain the data without the viewing privilege. **CVE ID : CVE-2022-29512**		
N/A	11-Jul-2022	4.3	Browsing restriction bypass vulnerability in Bulletin of Cybozu Garoon 4.0.0 to 5.9.1 allows a remote authenticated attacker to obtain the data of Bulletin. **CVE ID : CVE-2022-30943**	https://cs.cybozu.co.jp/2022/007682.html	A-CYB-GARO-200722/96
Affected Version(s): From (including) 4.10.0 Up to (including) 5.5.1					
Exposure of Resource to Wrong Sphere	04-Jul-2022	5.3	Improper authentication vulnerability in Scheduler of Cybozu Garoon 4.10.0 to 5.5.1 allows a remote attacker to obtain some data of Facility Information without logging in to the product. **CVE ID : CVE-2022-28713**	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/97
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jul-2022	4.8	Cross-site scripting vulnerability in Scheduler of Cybozu Garoon 4.10.0 to 5.5.1 allows a remote authenticated attacker with an administrative	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege to execute an arbitrary script. **CVE ID : CVE-2022-29513**		
Affected Version(s): From (including) 4.10.2 Up to (including) 5.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jul-2022	6.1	Cross-site scripting vulnerability in Organization's Information of Cybozu Garoon 4.10.2 to 5.5.1 allows a remote attacker to execute an arbitrary script on the logged-in user's web browser. **CVE ID : CVE-2022-27627**	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/99
Affected Version(s): From (including) 4.2.0 Up to (including) 5.5.1					
Exposure of Resource to Wrong Sphere	04-Jul-2022	4.3	Address information disclosure vulnerability in Cybozu Garoon 4.2.0 to 5.5.1 allows a remote authenticated attacker to obtain some data of Address. **CVE ID : CVE-2022-29467**	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/100
Affected Version(s): From (including) 4.6.0 Up to (including) 5.9.0					
Exposure of Resource to Wrong Sphere	04-Jul-2022	4.3	Browse restriction bypass vulnerability in Bulletin of Cybozu Garoon allows a remote authenticated attacker to obtain the data of Bulletin. **CVE ID : CVE-2022-29471**	https://cs.cybozu.co.jp/2022/007429.html	A-CYB-GARO-200722/101
Vendor: dainst					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cilantro					
Affected Version(s): * Up to (including) 0.0.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The dainst/cilantro repository through 0.0.4 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31531**	N/A	A-DAI-CILA-200722/102
Vendor: data_stream_algorithm_benchmark_project					
Product: data_stream_algorithm_benchmark					
Affected Version(s): * Up to (including) 2.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The DSABenchmark/DSAB repository through 2.1 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31567**	N/A	A-DAT-DATA-200722/103
Affected Version(s): * Up to (including) 2019-02-18					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	8.6	The DSAB-local/DSAB repository through 2019-02-18 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31566**	N/A	A-DAT-DATA-200722/104
Vendor: deep_learning_studio_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: deep_learning_studio					
Affected Version(s): 0.1.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The SummaLabs/DLS repository through 0.1.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31525**	N/A	A-DEE-DEEP-200722/105
Vendor: Dell					
Product: cloud_mobility_for_dell_emc_storage					
Affected Version(s): 1.3.0					
N/A	07-Jul-2022	9.8	Cloud Mobility for Dell EMC Storage, 1.3.0.XXX contains a RCE vulnerability. A non-privileged user could potentially exploit this vulnerability, leading to achieving a root shell. This is a critical issue; so Dell recommends customers to upgrade at the earliest opportunity. **CVE ID : CVE-2022-33936**	https://www.dell.com/support/kbdoc/en-us/000201258/dsa-2022-182-cloud-mobility-for-dell-emc-storage-security-update-for-a-path-traversal-rce-vulnerability	A-DEL-CLOU-200722/106
Product: powerprotect_cyber_recovery					
Affected Version(s): * Up to (excluding) 19.11					
Improper Privilege Management	07-Jul-2022	7.8	Dell PowerProtect Cyber Recovery, versions prior to 19.11, contain a privilege escalation vulnerability on	https://support.emc.com/kb/000201213	A-DEL-POWE-200722/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			virtual appliance deployments. A lower-privileged authenticated user can chain docker commands to escalate privileges to root leading to complete system takeover. **CVE ID : CVE-2022-32481**		
Vendor: denx					
Product: u-boot					
Affected Version(s): 2022.07					
Out-of-bounds Write	01-Jul-2022	7.8	Das U-Boot from v2020.10 to v2022.07-rc3 was discovered to contain an out-of-bounds write via the function sqfs_readdir(). **CVE ID : CVE-2022-33103**	https://lore.kernel.org/all/20220609140206.297405-1-miquel.raynal@bootlin.com/, https://lore.kernel.org/all/CALO=DHFB+yBoXxVr5KcsK0iFdg+e7ywko4-e+72kjbcS8JBfPw@mail.gmail.com/	A-DEN-U-BO-200722/108
Affected Version(s): From (including) 2020.10 Up to (excluding) 2022.07					
Out-of-bounds Write	01-Jul-2022	7.8	Das U-Boot from v2020.10 to v2022.07-rc3 was discovered to contain an out-of-bounds write via the function sqfs_readdir(). **CVE ID : CVE-2022-33103**	https://lore.kernel.org/all/20220609140206.297405-1-miquel.raynal@bootlin.com/, https://lore.kernel.org/all/CALO=DHFB+yBoXxVr5KcsK0iFdg+e7ywko4-	A-DEN-U-BO-200722/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				e+72kjbcS8JBfPw@mail.gmail.com/	
Vendor: devolutions					
Product: devolutions_server					
Affected Version(s): * Up to (excluding) 2022.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2022	5.4	HTML injection vulnerability in secure messages of Devolutions Server before 2022.2 allows attackers to alter the rendering of the page or redirect a user to another site. **CVE ID : CVE-2022-2316**	https://devolutions.net/security/advisories/DEVO-2022-0006	A-DEV-DEVO-200722/110
Affected Version(s): * Up to (excluding) 2022.2.0					
Incorrect Default Permissions	07-Jul-2022	8.8	Incorrect permission management in Devolutions Server before 2022.2 allows a new user with a preexisting username to inherit the permissions of that previous user. **CVE ID : CVE-2022-33996**	https://devolutions.net/security/advisories/DEVO-2022-0006, https://devolutions.net	A-DEV-DEVO-200722/111
Vendor: dice_project					
Product: dice					
Affected Version(s): 4.2.0					
Unrestricted Upload of File with Dangerous Type	05-Jul-2022	9.8	An arbitrary file upload vulnerability in Dice v4.2.0 allows attackers to execute arbitrary code via a crafted file.	N/A	A-DIC-DICE-200722/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32413		
Vendor: digitalguardian					
Product: digital_guardian					
Affected Version(s): 7.7.4.0042					
N/A	08-Jul-2022	5.1	Digital Guardian Agent 7.7.4.0042 allows an administrator (who ordinarily does not have a supported way to uninstall the product) to disable some of the agent functionality and then exfiltrate files to an external USB device. **CVE ID : CVE-2022-35412**	N/A	A-DIG-DIGI-200722/113
Vendor: Djangoproject					
Product: django					
Affected Version(s): From (including) 3.2 Up to (excluding) 3.2.14					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jul-2022	9.8	An issue was discovered in Django 3.2 before 3.2.14 and 4.0 before 4.0.6. The Trunc() and Extract() database functions are subject to SQL injection if untrusted data is used as a kind/lookup_name value. Applications that constrain the lookup name and kind choice to a known safe list are unaffected. **CVE ID : CVE-2022-34265**	https://www.djangoproject.com/weblog/2022/jul/04/security-releases/, https://docs.djangoproject.com/en/4.0/releases/security/	A-DJA-DJAN-200722/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.0 Up to (excluding) 4.0.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jul-2022	9.8	An issue was discovered in Django 3.2 before 3.2.14 and 4.0 before 4.0.6. The Trunc() and Extract() database functions are subject to SQL injection if untrusted data is used as a kind/lookup_name value. Applications that constrain the lookup name and kind choice to a known safe list are unaffected. **CVE ID : CVE-2022-34265**	https://www.djangoproject.com/weblog/2022/jul/04/security-releases/, https://docs.djangoproject.com/en/4.0/releases/security/	A-DJA-DJAN-200722/115
Vendor: Eclipse					
Product: jetty					
Affected Version(s): * Up to (excluding) 9.4.46					
Improper Input Validation	07-Jul-2022	2.7	In Eclipse Jetty versions 9.4.0 thru 9.4.46, and 10.0.0 thru 10.0.9, and 11.0.0 thru 11.0.9 versions, the parsing of the authority segment of an http scheme URI, the Jetty HttpURI class improperly detects an invalid input as a hostname. This can lead to failures in a Proxy scenario. **CVE ID : CVE-2022-2047**	https://github.com/eclipse/jetty.project/security/advisories/GHSA-cj7v-27pg-wf7q	A-ECL-JETT-200722/116
Affected Version(s): * Up to (excluding) 9.4.47					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	07-Jul-2022	7.5	In Eclipse Jetty HTTP/2 server implementation, when encountering an invalid HTTP/2 request, the error handling has a bug that can wind up not properly cleaning up the active connections and associated resources. This can lead to a Denial of Service scenario where there are no enough resources left to process good requests. **CVE ID : CVE-2022-2048**	https://github.com/eclipse/jetty.project/security/advisories/GHSA-wgmr-mf83-7x4j	A-ECL-JETT-200722/117
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.9					
Uncontrolled Resource Consumption	07-Jul-2022	7.5	In Eclipse Jetty HTTP/2 server implementation, when encountering an invalid HTTP/2 request, the error handling has a bug that can wind up not properly cleaning up the active connections and associated resources. This can lead to a Denial of Service scenario where there are no enough resources left to process good requests.	https://github.com/eclipse/jetty.project/security/advisories/GHSA-wgmr-mf83-7x4j	A-ECL-JETT-200722/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2048		
Improper Input Validation	07-Jul-2022	2.7	In Eclipse Jetty versions 9.4.0 thru 9.4.46, and 10.0.0 thru 10.0.9, and 11.0.0 thru 11.0.9 versions, the parsing of the authority segment of an http scheme URI, the Jetty HttpURI class improperly detects an invalid input as a hostname. This can lead to failures in a Proxy scenario. **CVE ID : CVE-2022-2047**	https://github.com/eclipse/jetty.project/security/advisories/GHSA-cj7v-27pg-wf7q	A-ECL-JETT-200722/119
Affected Version(s): From (including) 10.0.0 Up to (including) 10.0.9					
Improper Resource Shutdown or Release	07-Jul-2022	7.5	In Eclipse Jetty versions 10.0.0 thru 10.0.9, and 11.0.0 thru 11.0.9 versions, SslConnection does not release ByteBuffers from configured ByteBufferPool in case of error code paths. **CVE ID : CVE-2022-2191**	https://github.com/eclipse/jetty.project/security/advisories/GHSA-8mpp-f3f7-xc28	A-ECL-JETT-200722/120
Affected Version(s): From (including) 11.0.0 Up to (excluding) 11.0.9					
Uncontrolled Resource Consumption	07-Jul-2022	7.5	In Eclipse Jetty HTTP/2 server implementation, when encountering an invalid HTTP/2 request, the error handling has a bug that can wind up not	https://github.com/eclipse/jetty.project/security/advisories/GHSA-wgmr-mf83-7x4j	A-ECL-JETT-200722/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			properly cleaning up the active connections and associated resources. This can lead to a Denial of Service scenario where there are no enough resources left to process good requests. **CVE ID : CVE-2022-2048**		
Affected Version(s): From (including) 11.0.0 Up to (including) 11.0.9					
Improper Resource Shutdown or Release	07-Jul-2022	7.5	In Eclipse Jetty versions 10.0.0 thru 10.0.9, and 11.0.0 thru 11.0.9 versions, SslConnection does not release ByteBuffers from configured ByteBufferPool in case of error code paths. **CVE ID : CVE-2022-2191**	https://github.com/eclipse/jetty.project/security/advisories/GHSA-8mpp-f3f7-xc28	A-ECL-JETT-200722/122
Improper Input Validation	07-Jul-2022	2.7	In Eclipse Jetty versions 9.4.0 thru 9.4.46, and 10.0.0 thru 10.0.9, and 11.0.0 thru 11.0.9 versions, the parsing of the authority segment of an http scheme URI, the Jetty HttpURI class improperly detects an invalid input as a hostname. This can lead to failures in a Proxy scenario.	https://github.com/eclipse/jetty.project/security/advisories/GHSA-cj7v-27pg-wf7q	A-ECL-JETT-200722/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2047		
Vendor: Elastic					
Product: endpoint_security					
Affected Version(s): From (including) 7.13.0 Up to (including) 7.17.4					
Improper Privilege Management	06-Jul-2022	7.8	A local privilege escalation (LPE) issue was discovered in the ransomware canaries features of Elastic Endpoint Security for Windows, which could allow unprivileged users to elevate their privileges to those of the LocalSystem account. **CVE ID : CVE-2022-23714**	https://discuss.elastic.co/t/elastic-8-3-1-8-3-0-and-7-17-5-security-update/308613, https://www.elastic.co/community/security	A-ELA-ENDP-200722/124
Affected Version(s): From (including) 8.0.0 Up to (including) 8.2.3					
Improper Privilege Management	06-Jul-2022	7.8	A local privilege escalation (LPE) issue was discovered in the ransomware canaries features of Elastic Endpoint Security for Windows, which could allow unprivileged users to elevate their privileges to those of the LocalSystem account. **CVE ID : CVE-2022-23714**	https://discuss.elastic.co/t/elastic-8-3-1-8-3-0-and-7-17-5-security-update/308613, https://www.elastic.co/community/security	A-ELA-ENDP-200722/125
Product: kibana					
Affected Version(s): From (including) 8.0.0 Up to (including) 8.2.3					
Improper Neutralizat	06-Jul-2022	6.1	A cross-site-scripting (XSS) vulnerability	https://discuss.elastic.co/t/el	A-ELA-KIBA-200722/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			was discovered in the Vega Charts Kibana integration which could allow arbitrary JavaScript to be executed in a victim's browser. **CVE ID : CVE-2022-23713**	astic-8-3-1-8-3-0-and-7-17-5-security-update/308613, https://www.elastic.co/community/security	
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.17.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2022	6.1	A cross-site-scripting (XSS) vulnerability was discovered in the Vega Charts Kibana integration which could allow arbitrary JavaScript to be executed in a victim's browser. **CVE ID : CVE-2022-23713**	https://discuss.elastic.co/t/elastic-8-3-1-8-3-0-and-7-17-5-security-update/308613, https://www.elastic.co/community/security	A-ELA-KIBA-200722/127
Vendor: eqs					
Product: integrity_line					
Affected Version(s): * Up to (including) 2022-07-01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2022	6.1	EQS Integrity Line through 2022-07-01 allows a stored XSS via a crafted whistleblower entry. **CVE ID : CVE-2022-34007**	https://www.integrityline.com/	A-EQS-INTE-200722/128
Vendor: equanimity_project					
Product: equanimity					
Affected Version(s): * Up to (including) 2014-04-23					
Improper Limitation of a Pathname	11-Jul-2022	9.3	The AFDudley/equanimity repository through 2014-04-23 on	N/A	A-EQU-EQUA-200722/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31511**		
Vendor: fan_platform_project					
Product: fan_platform					
Affected Version(s): * Up to (including) 2021-04-20					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The Caoyongqi912/Fan_Platform repository through 2021-04-20 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31514**	N/A	A-FAN-FAN_-200722/130
Vendor: fishtank_project					
Product: fishtank					
Affected Version(s): * Up to (including) 2015-06-24					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The freefood89/Fishtank repository through 2015-06-24 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31535**	N/A	A-FIS-FISH-200722/131
Vendor: flask-file-server_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: flask-file-server					
Affected Version(s): * Up to (including) 2020-02-20					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The Wildog/flask-file-server repository through 2020-02-20 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31527**	N/A	A-FLA-FLAS-200722/132
Vendor: flask-mongo-skel_project					
Product: flask-mongo-skel					
Affected Version(s): * Up to (including) 2012-11-01					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The pleomax00/flask-mongo-skel repository through 2012-11-01 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31551**	N/A	A-FLA-FLAS-200722/133
Vendor: flask-mvc_project					
Product: flask-mvc					
Affected Version(s): * Up to (including) 2020-09-14					
Improper Limitation of a Pathname to a Restricted Directory	11-Jul-2022	9.3	The Atom02/flask-mvc repository through 2020-09-14 on GitHub allows absolute path traversal because the Flask send_file	N/A	A-FLA-FLAS-200722/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			function is used unsafely. **CVE ID : CVE-2022-31512**		
Vendor: flask-yeoman_project					
Product: flask-yeoman					
Affected Version(s): * Up to (including) 2013-09-13					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The tsileo/flask-yeoman repository through 2013-09-13 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31559**	N/A	A-FLA-FLAS-200722/135
Vendor: foxy-shop					
Product: foxyshop					
Affected Version(s): * Up to (excluding) 4.8.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2022	6.1	The FoxyShop WordPress plugin before 4.8.2 does not sanitise and escape a parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-1220**	N/A	A-FOX-FOXY-200722/136
Vendor: gallagher					
Product: command_centre					
Affected Version(s): * Up to (including) 8.20					
Improper Neutralization of Special	06-Jul-2022	5.5	Command Centre Server is vulnerable to SQL Injection via Windows Registry	https://security.gallagher.com/Security-	A-GAL-COMM-200722/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			settings for date fields on the server. The Windows Registry setting allows an attacker using the Visitor Management Kiosk, an application designed for public use, to invoke an arbitrary SQL query that has been preloaded into the registry of the Windows Server to obtain sensitive information. This issue affects: Gallagher Command Centre 8.60 versions prior to 8.60.1652; 8.50 versions prior to 8.50.2245; 8.40 versions prior to 8.40.2216; 8.30 versions prior to 8.30.1470; version 8.20 and prior versions. **CVE ID : CVE-2022-26348**	Advisories/CVE-2022-26348	
Affected Version(s): From (including) 8.30 Up to (excluding) 8.30.1470					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jul-2022	5.5	Command Centre Server is vulnerable to SQL Injection via Windows Registry settings for date fields on the server. The Windows Registry setting allows an attacker using the Visitor Management Kiosk, an application designed for public	https://security.gallagher.com/Security-Advisories/CVE-2022-26348	A-GAL-COMM-200722/138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use, to invoke an arbitrary SQL query that has been preloaded into the registry of the Windows Server to obtain sensitive information. This issue affects: Gallagher Command Centre 8.60 versions prior to 8.60.1652; 8.50 versions prior to 8.50.2245; 8.40 versions prior to 8.40.2216; 8.30 versions prior to 8.30.1470; version 8.20 and prior versions. **CVE ID : CVE-2022-26348**		
Affected Version(s): From (including) 8.40 Up to (excluding) 8.40.2216					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jul-2022	5.5	Command Centre Server is vulnerable to SQL Injection via Windows Registry settings for date fields on the server. The Windows Registry setting allows an attacker using the Visitor Management Kiosk, an application designed for public use, to invoke an arbitrary SQL query that has been preloaded into the registry of the Windows Server to obtain sensitive information. This	https://security.gallagher.com/Security-Advisories/CVE-2022-26348	A-GAL-COMM-200722/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects: Gallagher Command Centre 8.60 versions prior to 8.60.1652; 8.50 versions prior to 8.50.2245; 8.40 versions prior to 8.40.2216; 8.30 versions prior to 8.30.1470; version 8.20 and prior versions. **CVE ID : CVE-2022-26348**		
Affected Version(s): From (including) 8.50 Up to (excluding) 8.50.2245					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jul-2022	5.5	Command Centre Server is vulnerable to SQL Injection via Windows Registry settings for date fields on the server. The Windows Registry setting allows an attacker using the Visitor Management Kiosk, an application designed for public use, to invoke an arbitrary SQL query that has been preloaded into the registry of the Windows Server to obtain sensitive information. This issue affects: Gallagher Command Centre 8.60 versions prior to 8.60.1652; 8.50 versions prior to 8.50.2245; 8.40 versions prior to 8.40.2216; 8.30	https://security.gallagher.com/Security-Advisories/CVE-2022-26348	A-GAL-COMM-200722/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 8.30.1470; version 8.20 and prior versions. **CVE ID : CVE-2022-26348**		
Affected Version(s): From (including) 8.60 Up to (excluding) 8.60.1652					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jul-2022	5.5	Command Centre Server is vulnerable to SQL Injection via Windows Registry settings for date fields on the server. The Windows Registry setting allows an attacker using the Visitor Management Kiosk, an application designed for public use, to invoke an arbitrary SQL query that has been preloaded into the registry of the Windows Server to obtain sensitive information. This issue affects: Gallagher Command Centre 8.60 versions prior to 8.60.1652; 8.50 versions prior to 8.50.2245; 8.40 versions prior to 8.40.2216; 8.30 versions prior to 8.30.1470; version 8.20 and prior versions. **CVE ID : CVE-2022-26348**	https://security.gallagher.com/Security-Advisories/CVE-2022-26348	A-GAL-COMM-200722/141
Vendor: ganga_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ganga					
Affected Version(s): * Up to (excluding) 8.5.10					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The ganga-devs/ganga repository before 8.5.10 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31507**	https://github.com/ganga-devs/ganga/commit/730e7aba192407d35eb37dd7938d49071124be8c	A-GAN-GANG-200722/142
Vendor: getoutline					
Product: outline					
Affected Version(s): * Up to (excluding) 0.64.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository outline/outline prior to v0.64.4. **CVE ID : CVE-2022-2342**	https://github.com/outline/outline/commit/85657b7340cdeaa696034f294489df8d6a4914d3, https://huntr.dev/bounties/b2caceaa-5b28-40ba-9980-70144159efba	A-GET-OUTL-200722/143
Vendor: git-clone_project					
Product: git-clone					
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command	01-Jul-2022	9.8	All versions of package git-clone are vulnerable to Command Injection due to insecure usage of the --upload-pack feature of git.	https://gist.github.com/lirantal/9441f3a1212728476f7a6caa4acb2ccc, https://snyk.io/vuln/SNYK-	A-GIT-GIT--200722/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			**CVE ID : CVE-2022-25900**	JS-GITCLONE-2434308	
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): * Up to (excluding) 14.10.5					
Incorrect Permission Assignment for Critical Resource	01-Jul-2022	4.3	Improper access control in the runner jobs API in GitLab CE/EE affecting all versions prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows a previous maintainer of a project with a specific runner to access job and project meta data under certain conditions **CVE ID : CVE-2022-2227**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2227.json	A-GIT-GITL-200722/145
Affected Version(s): 15.1.0					
Incorrect Permission Assignment for Critical Resource	01-Jul-2022	9.8	A critical issue has been discovered in GitLab affecting all versions starting from 14.0 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 where it was possible for an unauthorised user to execute arbitrary code on the server using the project import feature. **CVE ID : CVE-2022-2185**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2185.json	A-GIT-GITL-200722/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	01-Jul-2022	7.5	An improper authorization issue in GitLab CE/EE affecting all versions from 13.7 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker to extract the value of an unprotected variable they know the name of in public projects or private projects they're a member of. **CVE ID : CVE-2022-2229**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2229.json	A-GIT-GITL-200722/147
N/A	01-Jul-2022	6.5	Information exposure in GitLab EE affecting all versions from 12.0 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker with the appropriate access tokens to obtain CI variables in a group with using IP-based access restrictions even if the GitLab Runner is calling from outside the allowed IP range **CVE ID : CVE-2022-2228**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2228.json, https://gitlab.com/gitlab-org/security/gitlab/-/issues/682	A-GIT-GITL-200722/148
URL Redirection to Untrusted Site ('Open Redirect')	01-Jul-2022	6.1	An open redirect vulnerability in GitLab EE/CE affecting all versions from 11.1 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows an	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2250.json	A-GIT-GITL-200722/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to redirect users to an arbitrary location if they trust the URL. **CVE ID : CVE-2022-2250**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jul-2022	5.4	Insufficient sanitization in GitLab EE's external issue tracker affecting all versions from 14.5 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker to perform cross-site scripting when a victim clicks on a maliciously crafted ZenTao link **CVE ID : CVE-2022-2235**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2235.json	A-GIT-GITL-200722/150
N/A	01-Jul-2022	5.3	A Regular Expression Denial of Service vulnerability in GitLab CE/EE affecting all versions from 1.0.2 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker to make a GitLab instance inaccessible via specially crafted web server response headers **CVE ID : CVE-2022-1954**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1954.json	A-GIT-GITL-200722/151
N/A	01-Jul-2022	5.3	An issue has been discovered in GitLab CE/EE affecting all	https://gitlab.com/gitlab-org/cves/-	A-GIT-GITL-200722/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions starting from 13.4 before 14.10.5, all versions starting from 15.0 before 15.0.4, all versions starting from 15.1 before 15.1.1. GitLab reveals if a user has enabled two-factor authentication on their account in the HTML source, to unauthenticated users. **CVE ID : CVE-2022-1963**	/blob/master/2022/CVE-2022-1963.json	
N/A	01-Jul-2022	5.3	An issue has been discovered in GitLab CE/EE affecting all versions from 8.13 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1. Under certain conditions, using the REST API an unprivileged user was able to change labels description. **CVE ID : CVE-2022-1999**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1999.json	A-GIT-GITL-200722/153
Incorrect Default Permissions	01-Jul-2022	5.3	An issue has been discovered in GitLab affecting all versions starting from 12.4 before 14.10.5, all versions starting from 15.0 before 15.0.4, all versions starting from 15.1 before 15.1.1. GitLab was leaking Conan packages names due to	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2270.json	A-GIT-GITL-200722/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incorrect permissions verification. **CVE ID : CVE-2022-2270**		
N/A	01-Jul-2022	5.3	An information disclosure vulnerability in GitLab EE affecting all versions from 12.5 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows disclosure of release titles if group milestones are associated with any project releases. **CVE ID : CVE-2022-2281**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2281.json	A-GIT-GITL-200722/155
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jul-2022	4.8	A Stored Cross-Site Scripting vulnerability in the project settings page in GitLab CE/EE affecting all versions from 14.4 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows an attacker to execute arbitrary JavaScript code in GitLab on a victim's behalf. **CVE ID : CVE-2022-2230**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2230.json	A-GIT-GITL-200722/156
Exposure of Resource to Wrong Sphere	01-Jul-2022	4.3	Incorrect authorization in GitLab EE affecting all versions from 10.7 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1,	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1983.json	A-GIT-GITL-200722/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed an attacker already in possession of a valid Deploy Key or a Deploy Token to misuse it from any location to access Container Registries even when IP address restrictions were configured. **CVE ID : CVE-2022-1983**		
Incorrect Permission Assignment for Critical Resource	01-Jul-2022	4.3	Improper access control in the runner jobs API in GitLab CE/EE affecting all versions prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows a previous maintainer of a project with a specific runner to access job and project meta data under certain conditions **CVE ID : CVE-2022-2227**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2227.json	A-GIT-GITL-200722/158
Incorrect Authorization	01-Jul-2022	4.3	An access control vulnerability in GitLab EE/CE affecting all versions from 14.8 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows authenticated users to enumerate issues in non-linked sentry projects. **CVE ID : CVE-2022-2243**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2243.json	A-GIT-GITL-200722/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	01-Jul-2022	4.3	An improper authorization vulnerability in GitLab EE/CE affecting all versions from 14.8 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows project memebers with reporter role to manage issues in project's error tracking feature. **CVE ID : CVE-2022-2244**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2244.json	A-GIT-GITL-200722/160
Incorrect Authorization	01-Jul-2022	2.7	An issue has been discovered in GitLab EE affecting all versions starting from 12.2 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1. In GitLab, if a group enables the setting to restrict access to users belonging to specific domains, that allow-list may be bypassed if a Maintainer uses the 'Invite a group' feature to invite a group that has members that don't comply with domain allow-list. **CVE ID : CVE-2022-1981**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1981.json	A-GIT-GITL-200722/161
Affected Version(s): From (including) 1.0.2 Up to (excluding) 14.10.5					
N/A	01-Jul-2022	5.3	A Regular Expression Denial of Service	https://gitlab.com/gitlab-	A-GIT-GITL-200722/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in GitLab CE/EE affecting all versions from 1.0.2 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker to make a GitLab instance inaccessible via specially crafted web server response headers **CVE ID : CVE-2022-1954**	org/cves/-/blob/master/2022/CVE-2022-1954.json	
Affected Version(s): From (including) 10.7.0 Up to (excluding) 14.10.5					
Exposure of Resource to Wrong Sphere	01-Jul-2022	4.3	Incorrect authorization in GitLab EE affecting all versions from 10.7 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allowed an attacker already in possession of a valid Deploy Key or a Deploy Token to misuse it from any location to access Container Registries even when IP address restrictions were configured. **CVE ID : CVE-2022-1983**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1983.json	A-GIT-GITL-200722/163
Affected Version(s): From (including) 11.1.0 Up to (excluding) 14.0.5					
URL Redirection to Untrusted Site ('Open Redirect')	01-Jul-2022	6.1	An open redirect vulnerability in GitLab EE/CE affecting all versions from 11.1 prior to 14.10.5, 15.0 prior to	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-	A-GIT-GITL-200722/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.0.4, and 15.1 prior to 15.1.1, allows an attacker to redirect users to an arbitrary location if they trust the URL. **CVE ID : CVE-2022-2250**	2022-2250.json	
Affected Version(s): From (including) 11.1.0 Up to (excluding) 14.10.5					
URL Redirection to Untrusted Site ('Open Redirect')	01-Jul-2022	6.1	An open redirect vulnerability in GitLab EE/CE affecting all versions from 11.1 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows an attacker to redirect users to an arbitrary location if they trust the URL. **CVE ID : CVE-2022-2250**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2250.json	A-GIT-GITL-200722/165
Affected Version(s): From (including) 12.0.0 Up to (excluding) 14.10.5					
N/A	01-Jul-2022	6.5	Information exposure in GitLab EE affecting all versions from 12.0 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker with the appropriate access tokens to obtain CI variables in a group with using IP-based access restrictions even if the GitLab Runner is calling from outside the allowed IP range	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2228.json, https://gitlab.com/gitlab-org/security/gitlab/-/issues/682	A-GIT-GITL-200722/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2228		
Affected Version(s): From (including) 12.2.0 Up to (excluding) 14.10.5					
Incorrect Authorization	01-Jul-2022	2.7	An issue has been discovered in GitLab EE affecting all versions starting from 12.2 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1. In GitLab, if a group enables the setting to restrict access to users belonging to specific domains, that allow-list may be bypassed if a Maintainer uses the 'Invite a group' feature to invite a group that has members that don't comply with domain allow-list. **CVE ID : CVE-2022-1981**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1981.json	A-GIT-GITL-200722/167
Affected Version(s): From (including) 12.4.0 Up to (excluding) 14.10.5					
Incorrect Default Permissions	01-Jul-2022	5.3	An issue has been discovered in GitLab affecting all versions starting from 12.4 before 14.10.5, all versions starting from 15.0 before 15.0.4, all versions starting from 15.1 before 15.1.1. GitLab was leaking Conan packages names due to incorrect permissions verification.	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2270.json	A-GIT-GITL-200722/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2270		
Affected Version(s): From (including) 12.5.0 Up to (excluding) 14.10.5					
N/A	01-Jul-2022	5.3	An information disclosure vulnerability in GitLab EE affecting all versions from 12.5 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows disclosure of release titles if group milestones are associated with any project releases. **CVE ID : CVE-2022-2281**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2281.json	A-GIT-GITL-200722/169
Affected Version(s): From (including) 13.4.0 Up to (excluding) 14.10.5					
N/A	01-Jul-2022	5.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.4 before 14.10.5, all versions starting from 15.0 before 15.0.4, all versions starting from 15.1 before 15.1.1. GitLab reveals if a user has enabled two-factor authentication on their account in the HTML source, to unauthenticated users. **CVE ID : CVE-2022-1963**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1963.json	A-GIT-GITL-200722/170
Affected Version(s): From (including) 13.7.0 Up to (excluding) 14.10.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	01-Jul-2022	7.5	An improper authorization issue in GitLab CE/EE affecting all versions from 13.7 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker to extract the value of an unprotected variable they know the name of in public projects or private projects they're a member of. **CVE ID : CVE-2022-2229**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2229.json	A-GIT-GITL-200722/171
Affected Version(s): From (including) 14.0.0 Up to (excluding) 14.10.5					
Incorrect Permission Assignment for Critical Resource	01-Jul-2022	9.8	A critical issue has been discovered in GitLab affecting all versions starting from 14.0 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 where it was possible for an unauthorised user to execute arbitrary code on the server using the project import feature. **CVE ID : CVE-2022-2185**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2185.json	A-GIT-GITL-200722/172
Affected Version(s): From (including) 14.0.0 Up to (excluding) 14.4.5					
Improper Neutralization of Input During Web Page Generation	01-Jul-2022	6.1	An issue has been discovered in GitLab affecting all versions starting from 14.0 before 14.4.5, all versions starting from 14.5.0 before 14.5.3,	https://gitlab.com/gitlab-org/gitlab/-/issues/339146, https://gitlab.com/gitlab-	A-GIT-GITL-200722/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			all versions starting from 14.6.0 before 14.6.2. GitLab was not disabling the Autocomplete attribute of fields related to sensitive information making it possible to be retrieved under certain conditions. **CVE ID : CVE-2022-0167**	org/cves/-/blob/master/2022/CVE-2022-0167.json	
Affected Version(s): From (including) 14.4.0 Up to (excluding) 14.10.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jul-2022	4.8	A Stored Cross-Site Scripting vulnerability in the project settings page in GitLab CE/EE affecting all versions from 14.4 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows an attacker to execute arbitrary JavaScript code in GitLab on a victim's behalf. **CVE ID : CVE-2022-2230**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2230.json	A-GIT-GITL-200722/174
Affected Version(s): From (including) 14.5.0 Up to (excluding) 14.10.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jul-2022	5.4	Insufficient sanitization in GitLab EE's external issue tracker affecting all versions from 14.5 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker to perform cross-site scripting when a	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2235.json	A-GIT-GITL-200722/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim clicks on a maliciously crafted ZenTao link **CVE ID : CVE-2022-2235**		
Affected Version(s): From (including) 14.5.0 Up to (excluding) 14.5.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jul-2022	6.1	An issue has been discovered in GitLab affecting all versions starting from 14.0 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was not disabling the Autocomplete attribute of fields related to sensitive information making it possible to be retrieved under certain conditions. **CVE ID : CVE-2022-0167**	https://gitlab.com/gitlab-org/gitlab/-/issues/339146, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0167.json	A-GIT-GITL-200722/176
Affected Version(s): From (including) 14.6.0 Up to (excluding) 14.6.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jul-2022	6.1	An issue has been discovered in GitLab affecting all versions starting from 14.0 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was not disabling the Autocomplete attribute of fields related to sensitive information making it	https://gitlab.com/gitlab-org/gitlab/-/issues/339146, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0167.json	A-GIT-GITL-200722/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible to be retrieved under certain conditions. **CVE ID : CVE-2022-0167**		
Affected Version(s): From (including) 14.8.0 Up to (excluding) 14.10.5					
Incorrect Authorization	01-Jul-2022	4.3	An access control vulnerability in GitLab EE/CE affecting all versions from 14.8 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows authenticated users to enumerate issues in non-linked sentry projects. **CVE ID : CVE-2022-2243**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2243.json	A-GIT-GITL-200722/178
Incorrect Authorization	01-Jul-2022	4.3	An improper authorization vulnerability in GitLab EE/CE affecting all versions from 14.8 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows project memebers with reporter role to manage issues in project's error tracking feature. **CVE ID : CVE-2022-2244**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2244.json	A-GIT-GITL-200722/179
Affected Version(s): From (including) 15.0.0 Up to (excluding) 15.0.4					
Incorrect Permission Assignment for	01-Jul-2022	9.8	A critical issue has been discovered in GitLab affecting all versions starting from	https://gitlab.com/gitlab-org/cves/-/blob/master/	A-GIT-GITL-200722/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			14.0 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 where it was possible for an unauthorised user to execute arbitrary code on the server using the project import feature. **CVE ID : CVE-2022-2185**	2022/CVE-2022-2185.json	
Incorrect Authorization	01-Jul-2022	7.5	An improper authorization issue in GitLab CE/EE affecting all versions from 13.7 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker to extract the value of an unprotected variable they know the name of in public projects or private projects they're a member of. **CVE ID : CVE-2022-2229**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2229.json	A-GIT-GITL-200722/181
N/A	01-Jul-2022	6.5	Information exposure in GitLab EE affecting all versions from 12.0 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker with the appropriate access tokens to obtain CI variables in a group with using IP-based access restrictions even if the GitLab Runner is	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2228.json, https://gitlab.com/gitlab-org/security/gitlab/-/issues/682	A-GIT-GITL-200722/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calling from outside the allowed IP range **CVE ID : CVE-2022-2228**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Jul-2022	6.1	An open redirect vulnerability in GitLab EE/CE affecting all versions from 11.1 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows an attacker to redirect users to an arbitrary location if they trust the URL. **CVE ID : CVE-2022-2250**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2250.json	A-GIT-GITL-200722/183
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jul-2022	5.4	Insufficient sanitization in GitLab EE's external issue tracker affecting all versions from 14.5 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker to perform cross-site scripting when a victim clicks on a maliciously crafted ZenTao link **CVE ID : CVE-2022-2235**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2235.json	A-GIT-GITL-200722/184
N/A	01-Jul-2022	5.3	A Regular Expression Denial of Service vulnerability in GitLab CE/EE affecting all versions from 1.0.2 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1954.json	A-GIT-GITL-200722/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to 15.1.1 allows an attacker to make a GitLab instance inaccessible via specially crafted web server response headers **CVE ID : CVE-2022-1954**		
N/A	01-Jul-2022	5.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.4 before 14.10.5, all versions starting from 15.0 before 15.0.4, all versions starting from 15.1 before 15.1.1. GitLab reveals if a user has enabled two-factor authentication on their account in the HTML source, to unauthenticated users. **CVE ID : CVE-2022-1963**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1963.json	A-GIT-GITL-200722/186
N/A	01-Jul-2022	5.3	An issue has been discovered in GitLab CE/EE affecting all versions from 8.13 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1. Under certain conditions, using the REST API an unprivileged user was able to change labels description.	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1999.json	A-GIT-GITL-200722/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1999		
Incorrect Default Permissions	01-Jul-2022	5.3	An issue has been discovered in GitLab affecting all versions starting from 12.4 before 14.10.5, all versions starting from 15.0 before 15.0.4, all versions starting from 15.1 before 15.1.1. GitLab was leaking Conan packages names due to incorrect permissions verification. **CVE ID : CVE-2022-2270**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2270.json	A-GIT-GITL-200722/188
N/A	01-Jul-2022	5.3	An information disclosure vulnerability in GitLab EE affecting all versions from 12.5 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows disclosure of release titles if group milestones are associated with any project releases. **CVE ID : CVE-2022-2281**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2281.json	A-GIT-GITL-200722/189
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jul-2022	4.8	A Stored Cross-Site Scripting vulnerability in the project settings page in GitLab CE/EE affecting all versions from 14.4 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2230.json	A-GIT-GITL-200722/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to 15.1.1, allows an attacker to execute arbitrary JavaScript code in GitLab on a victim's behalf. **CVE ID : CVE-2022-2230**		
Exposure of Resource to Wrong Sphere	01-Jul-2022	4.3	Incorrect authorization in GitLab EE affecting all versions from 10.7 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allowed an attacker already in possession of a valid Deploy Key or a Deploy Token to misuse it from any location to access Container Registries even when IP address restrictions were configured. **CVE ID : CVE-2022-1983**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1983.json	A-GIT-GITL-200722/191
Incorrect Permission Assignment for Critical Resource	01-Jul-2022	4.3	Improper access control in the runner jobs API in GitLab CE/EE affecting all versions prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows a previous maintainer of a project with a specific runner to access job and project meta data under certain conditions **CVE ID : CVE-2022-2227**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2227.json	A-GIT-GITL-200722/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	01-Jul-2022	4.3	An access control vulnerability in GitLab EE/CE affecting all versions from 14.8 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows authenticated users to enumerate issues in non-linked sentry projects. **CVE ID : CVE-2022-2243**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2243.json	A-GIT-GITL-200722/193
Incorrect Authorization	01-Jul-2022	4.3	An improper authorization vulnerability in GitLab EE/CE affecting all versions from 14.8 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows project memebers with reporter role to manage issues in project's error tracking feature. **CVE ID : CVE-2022-2244**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2244.json	A-GIT-GITL-200722/194
Incorrect Authorization	01-Jul-2022	2.7	An issue has been discovered in GitLab EE affecting all versions starting from 12.2 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1. In GitLab, if a group enables the setting to restrict access to users belonging to specific domains, that allow-	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1981.json	A-GIT-GITL-200722/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			list may be bypassed if a Maintainer uses the 'Invite a group' feature to invite a group that has members that don't comply with domain allow-list. **CVE ID : CVE-2022-1981**		
Affected Version(s): From (including) 8.13.0 Up to (excluding) 14.10.5					
N/A	01-Jul-2022	5.3	An issue has been discovered in GitLab CE/EE affecting all versions from 8.13 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1. Under certain conditions, using the REST API an unprivileged user was able to change labels description. **CVE ID : CVE-2022-1999**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1999.json	A-GIT-GITL-200722/196
Vendor: glance_project					
Product: glance					
Affected Version(s): * Up to (including) 2014-06-27					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The nlpweb/glance repository through 2014-06-27 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31546**	N/A	A-GLA-GLAN-200722/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Gnupg					
Product: gnupg					
Affected Version(s): * Up to (including) 2.3.6					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-Jul-2022	6.5	GnuPG through 2.3.6, in unusual situations where an attacker possesses any secret-key information from a victim's keyring and other constraints (e.g., use of GPGME) are met, allows signature forgery via injection into the status line. **CVE ID : CVE-2022-34903**	https://dev.gnupg.org/T6027, https://bugs.debian.org/1014157	A-GNU-GNUP-200722/198
Vendor: golem_project					
Product: golem					
Affected Version(s): * Up to (including) 2016-05-17					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The seveas/golem repository through 2016-05-17 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31557**	N/A	A-GOL-GOLE-200722/199
Vendor: H3C					
Product: ssl_vpn					
Affected Version(s): * Up to (including) 2022-07-10					
Improper Neutralization of Input During	11-Jul-2022	6.1	H3C SSL VPN through 2022-07-10 allows wnm/login/login.json svpnlang cookie XSS.	N/A	A-H3C-SSL_-200722/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2022-35416**		
Vendor: harveyzyh_python_project					
Product: harveyzyh_python					
Affected Version(s): * Up to (including) 2022-05-04					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The Harveyzyh/Python repository through 2022-05-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31516**	N/A	A-HAR-HARV-200722/201
Vendor: Haxx					
Product: curl					
Affected Version(s): * Up to (excluding) 7.84.0					
Incorrect Default Permissions	07-Jul-2022	9.8	When curl < 7.84.0 saves cookies, alt-svc and hsts data to local files, it makes the operation atomic by finalizing the operation with a rename from a temporary name to the final target file name.In that rename operation, it might accidentally *widen* the permissions for the target file, leaving the updated file accessible to more users than intended.	N/A	A-HAX-CURL-200722/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32207		
Allocation of Resources Without Limits or Throttling	07-Jul-2022	6.5	curl < 7.84.0 supports "chained" HTTP compression algorithms, meaning that a serverresponse can be compressed multiple times and potentially with different algorithms. The number of acceptable "links" in this "decompression chain" was unbounded, allowing a malicious server to insert a virtually unlimited number of compression steps.The use of such a decompression chain could result in a "malloc bomb", makingcurl end up spending enormous amounts of allocated heap memory, or trying toand returning out of memory errors. **CVE ID : CVE-2022-32206**	N/A	A-HAX-CURL-200722/203
Allocation of Resources Without Limits or Throttling	07-Jul-2022	4.3	A malicious server can serve excessive amounts of `Set-Cookie:` headers in a HTTP response to curl and curl < 7.84.0 stores all of them. A sufficiently large amount of (big) cookies make	N/A	A-HAX-CURL-200722/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			subsequent HTTP requests to this, or other servers to which the cookies match, create requests that become larger than the threshold that curl uses internally to avoid sending crazy large requests (1048576 bytes) and instead returns an error.This denial state might remain for as long as the same cookies are kept, match and haven't expired. Due to cookie matching rules, a server on `foo.example.com` can set cookies that also would match for `bar.example.com`, making it it possible for a "sister server" to effectively cause a denial of service for a sibling site on the same second level domain using this method. **CVE ID : CVE-2022-32205**		
Affected Version(s): From (including) 7.16.4 Up to (excluding) 7.84.0					
Out-of-bounds Write	07-Jul-2022	5.9	When curl < 7.84.0 does FTP transfers secured by krb5, it handles message verification failures wrongly. This flaw makes it possible for	N/A	A-HAX-CURL-200722/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a Man-In-The-Middle attack to go unnoticed and even allows it to inject data to the client. **CVE ID : CVE-2022-32208**		
Vendor: hcltechsw					
Product: hcl_launch					
Affected Version(s): 7.0.5.10					
Insufficiently Protected Credentials	06-Jul-2022	5.5	HCL Launch stores user credentials in plain clear text which can be read by a local user. **CVE ID : CVE-2022-27548**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0099253	A-HCL-HCL_-200722/206
Insertion of Sensitive Information into Log File	06-Jul-2022	5.5	HCL Launch may store certain data for recurring activities in a plain text format. **CVE ID : CVE-2022-27549**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0099254	A-HCL-HCL_-200722/207
Affected Version(s): 7.1.2.6					
Insufficiently Protected Credentials	06-Jul-2022	5.5	HCL Launch stores user credentials in plain clear text which can be read by a local user. **CVE ID : CVE-2022-27548**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0099253	A-HCL-HCL_-200722/208
Insertion of Sensitive Information into Log File	06-Jul-2022	5.5	HCL Launch may store certain data for recurring activities in a plain text format. **CVE ID : CVE-2022-27549**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0099254	A-HCL-HCL_-200722/209
Affected Version(s): 7.2.2.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	06-Jul-2022	5.5	HCL Launch stores user credentials in plain clear text which can be read by a local user. **CVE ID : CVE-2022-27548**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0099253	A-HCL-HCL_-200722/210
Insertion of Sensitive Information into Log File	06-Jul-2022	5.5	HCL Launch may store certain data for recurring activities in a plain text format. **CVE ID : CVE-2022-27549**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0099254	A-HCL-HCL_-200722/211
Vendor: helm-flask-celery_project					
Product: helm-flask-celery					
Affected Version(s): * Up to (including) 2022-05-25					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The olmax99/helm-flask-celery repository before 2022-05-25 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31549**	https://github.com/olmax99/helm-flask-celery/commit/28c985d712d7ac26893433e8035e2e3678fcae9f	A-HEL-HELM-200722/212
Vendor: heroiclabs					
Product: nakama					
Affected Version(s): * Up to (excluding) 3.13.0					
Improper Restriction of Excessive Authentication Attempts	05-Jul-2022	9.8	Improper Restriction of Excessive Authentication Attempts in GitHub repository heroiclabs/nakama prior to 3.13.0. This results in login brute-force attacks.	https://huntr.dev/bounties/3055b3f5-6b80-4d47-8e00-3500dfb458bc, https://github.com/heroiclabs/nakama/com	A-HER-NAKA-200722/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2321	mit/e2e02fce80ff33ce45f8a6ebc0b7a99ee0b03824	
Insufficient Session Expiration	05-Jul-2022	7.5	Old session tokens can be used to authenticate to the application and send authenticated requests. **CVE ID : CVE-2022-2306**	https://github.com/heroiclabs/nakama/commit/ce8d3921e2acd44ef8b5e6edfe595b6df067b166, https://huntr.dev/bounties/35acf263-6db4-4310-ab27-4c3c3a53f796	A-HER-NAKA-200722/214
Vendor: Hex-rays					
Product: ida					
Affected Version(s): 6.6					
Out-of-bounds Write	07-Jul-2022	5.5	A memory corruption in Hex Rays Ida Pro v6.6 allows attackers to cause a Denial of Service (DoS) via a crafted file. Related to Data from Faulting Address controls subsequent Write Address starting at msvcrt!memcpy+0x0000000000000056. **CVE ID : CVE-2022-32441**	N/A	A-HEX-IDA-200722/215
Vendor: hin-eng-preprocessing_project					
Product: hin-eng-preprocessing					
Affected Version(s): * Up to (including) 2019-07-16					
Improper Limitation of a	11-Jul-2022	9.3	The kumardeepak/hin-eng-preprocessing	N/A	A-HIN-HIN--200722/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			repository through 2019-07-16 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31540**		
Vendor: homepage_project					
Product: homepage					
Affected Version(s): * Up to (including) 2017-03-06					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The nrlakin/homepage repository through 2017-03-06 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31548**	N/A	A-HOM-HOME-200722/217
Vendor: home__internet_project					
Product: home__internet					
Affected Version(s): * Up to (including) 2020-08-28					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The umeshpatil-dev/Home__internet repository through 2020-08-28 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31585**	N/A	A-HOM-HOME-200722/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: hongcms_project					
Product: hongcms					
Affected Version(s): 3.0.0					
N/A	01-Jul-2022	7.2	An issue in the languages config file of HongCMS v3.0 allows attackers to getshell. **CVE ID : CVE-2022-32411**	N/A	A-HON-HONG-200722/219
N/A	01-Jul-2022	7.2	An issue in the /template/edit component of HongCMS v3.0 allows attackers to getshell. **CVE ID : CVE-2022-32412**	N/A	A-HON-HONG-200722/220
Vendor: hospital_management_system_project					
Product: hospital_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Jul-2022	9.8	Hospital Management System v1.0 was discovered to contain a SQL injection vulnerability via the loginid parameter at adminlogin.php. **CVE ID : CVE-2022-32093**	N/A	A-HOS-HOSP-200722/221
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Jul-2022	9.8	Hospital Management System v1.0 was discovered to contain a SQL injection vulnerability via the loginid parameter at doctorlogin.php. **CVE ID : CVE-2022-32094**	N/A	A-HOS-HOSP-200722/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Jul-2022	9.8	Hospital Management System v1.0 was discovered to contain a SQL injection vulnerability via the editid parameter at orders.php. **CVE ID : CVE-2022-32095**	N/A	A-HOS-HOSP-200722/223
Vendor: hotel_management_system_project					
Product: hotel_management_system					
Affected Version(s): 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-2022	5.4	A vulnerability was found in SourceCodester Hotel Management System 2.0. It has been rated as problematic. This issue affects some unknown processing of the file /ci_hms/search of the component Search. The manipulation of the argument search with the input "><script>alert("XSS")</script> leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2022-2291**	N/A	A-HOT-HOTE-200722/224
Improper Neutralization of Input	12-Jul-2022	5.4	A vulnerability classified as problematic has been found in	N/A	A-HOT-HOTE-200722/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			SourceCodester Hotel Management System 2.0. Affected is an unknown function of the file /ci_hms/massage_room/edit/1 of the component Room Edit Page. The manipulation of the argument massageroomDetails with the input "><script>alert("XSS")</script> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2022-2292**		
Vendor: Humhub					
Product: humhub					
Affected Version(s): * Up to (excluding) 1.10.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2022	4.8	HumHub is an Open Source Enterprise Social Network. Affected versions of HumHub are vulnerable to a stored Cross-Site Scripting (XSS) vulnerability. For exploitation, the attacker would need a permission to administer the Spaces feature. The names of individual "spaces" are not properly	https://github.com/humhub/humhub/commit/07d9f8f9b6334970ee38156a3416c3708d157cae, https://github.com/humhub/humhub/commit/f88991dfe56a05870df165ac89a2755dd4c1ffa1, https://github.	A-HUM-HUMH-200722/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escaped and so an attacker with sufficient privilege could insert malicious javascript into a space name and exploit system users who visit that space. It is recommended that the HumHub is upgraded to 1.11.4, 1.10.5. There are no known workarounds for this issue. **CVE ID : CVE-2022-31133**	com/humhub/humhub/security/advisories/GHSA-p7h3-73v7-959c	
Affected Version(s): From (including) 1.11.0 Up to (excluding) 1.11.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2022	4.8	HumHub is an Open Source Enterprise Social Network. Affected versions of HumHub are vulnerable to a stored Cross-Site Scripting (XSS) vulnerability. For exploitation, the attacker would need a permission to administer the Spaces feature. The names of individual "spaces" are not properly escaped and so an attacker with sufficient privilege could insert malicious javascript into a space name and exploit system users who visit that space. It is recommended that the HumHub is upgraded to 1.11.4,	https://github.com/humhub/humhub/commit/07d9f8f9b6334970ee38156a3416c3708d157cae, https://github.com/humhub/humhub/commit/f88991dfe56a05870df165ac89a2755dd4c1ffa1, https://github.com/humhub/humhub/security/advisories/GHSA-p7h3-73v7-959c	A-HUM-HUMH-200722/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.10.5. There are no known workarounds for this issue. **CVE ID : CVE-2022-31133**		
Vendor: hyperledger					
Product: fabric					
Affected Version(s): * Up to (excluding) 2.2.7					
Improper Input Validation	07-Jul-2022	7.5	Hyperledger Fabric is a permissioned distributed ledger framework. In affected versions if a consensus client sends a malformed consensus request to an orderer it may crash the orderer node. A fix has been added in commit 0f1835949 which checks for missing consensus messages and returns an error to the consensus client should the message be missing. Users are advised to upgrade to versions 2.2.7 or v2.4.5. There are no known workarounds for this issue. **CVE ID : CVE-2022-31121**	https://github.com/hyperledger/fabric/commit/0f183594 93bcbd5f9f9d1 a9b05adabfe5 da23b06, https://github.com/hyperledger/fabric/security/advisories/GHSA-72x4-cq6r-jp4p	A-HYP-FABR-200722/228
Affected Version(s): From (including) 2.3.0 Up to (excluding) 2.4.5					
Improper Input Validation	07-Jul-2022	7.5	Hyperledger Fabric is a permissioned distributed ledger framework. In affected versions if a	https://github.com/hyperledger/fabric/commit/0f183594 93bcbd5f9f9d1	A-HYP-FABR-200722/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consensus client sends a malformed consensus request to an orderer it may crash the orderer node. A fix has been added in commit 0f1835949 which checks for missing consensus messages and returns an error to the consensus client should the message be missing. Users are advised to upgrade to versions 2.2.7 or v2.4.5. There are no known workarounds for this issue. **CVE ID : CVE-2022-31121**	a9b05adabfe5da23b06, https://github.com/hyperledger/fabric/security/advisories/GHSA-72x4-cq6r-jp4p	
Vendor: iasset_project					
Product: iasset					
Affected Version(s): * Up to (including) 2022-05-04					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The ralphjzhang/iasset repository through 2022-05-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31579**	N/A	A-IAS-IASS-200722/230
Vendor: IBM					
Product: app_connect_enterprise_certified_container					
Affected Version(s): 4.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jul-2022	4.9	IBM App Connect Enterprise Certified Container 4.2 could allow a user from the administration console to cause a denial of service by creating a specially crafted request. IBM X-Force ID: 228221. **CVE ID : CVE-2022-31770**	https://www.ibm.com/support/pages/node/6601125, https://exchange.xforce.ibmcloud.com/vulnerabilities/228221	A-IBM-APP_-200722/231
Product: cics_tx					
Affected Version(s): 11.1					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Jul-2022	5.4	IBM CICS TX Standard and Advanced 11.1 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 229330. **CVE ID : CVE-2022-34160**	https://www.ibm.com/support/pages/node/6601555, https://www.ibm.com/support/pages/node/6601553, https://exchange.xforce.ibmcloud.com/vulnerabilities/229330	A-IBM-CICS-200722/232
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2022	5.4	IBM CICS TX Standard and Advanced 11.1 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	https://www.ibm.com/support/pages/node/6601609, https://www.ibm.com/support/pages/node/6601579	A-IBM-CICS-200722/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session. IBM X-Force ID: 229430. **CVE ID : CVE-2022-34166**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2022	5.4	IBM CICS TX Standard and Advanced 11.1 is vulnerable to stored 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: 229432. **CVE ID : CVE-2022-34167**	https://www.ibm.com/support/pages/node/6601655, https://exchange.xforce.ibmcloud.com/vulnerabilities/229432, https://www.ibm.com/support/pages/node/6601657	A-IBM-CICS-200722/234
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Jul-2022	5.4	IBM CICS TX Standard and Advanced 11.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 229435. **CVE ID : CVE-2022-34306**	https://exchange.xforce.ibmcloud.com/vulnerabilities/229435, https://www.ibm.com/support/pages/node/6601663, https://www.ibm.com/support/pages/node/6601659	A-IBM-CICS-200722/235
Product: infosphere_information_server					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 11.7					
Missing Authorization	01-Jul-2022	5.4	An improper validation vulnerability in IBM InfoSphere Information Server 11.7 Pack for SAP Apps and BW Packs may lead to creation of directories and files on the server file system that may contain non-sensitive debugging information like stack traces. IBM X-Force ID: 221323. **CVE ID : CVE-2022-22373**	https://exchange.xforce.ibmcloud.com/vulnerabilities/221323, https://www.ibm.com/support/pages/node/6600235	A-IBM-INFO-200722/236
Product: open_liberty					
Affected Version(s): -					
Authentication Bypass by Spoofing	08-Jul-2022	8.8	IBM WebSphere Application Server Liberty 17.0.0.3 through 22.0.0.7 and Open Liberty are vulnerable to identity spoofing by an authenticated user using a specially crafted request. IBM X-Force ID: 225604. **CVE ID : CVE-2022-22476**	https://www.ibm.com/support/pages/node/6602015, https://exchange.xforce.ibmcloud.com/vulnerabilities/225604	A-IBM-OPEN-200722/237
Product: security_verify_access					
Affected Version(s): 10.0.0.0					
N/A	08-Jul-2022	7.8	IBM Security Access Manager Appliance 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 could allow a local	https://www.ibm.com/support/pages/node/6601729, https://exchan	A-IBM-SECU-200722/238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user to obtain elevated privileges due to improper access permissions. IBM X-Force ID: 225082. **CVE ID : CVE-2022-22465**	ge.xforce.ibmcloud.com/vulnerabilities/225082	
Inadequate Encryption Strength	08-Jul-2022	7.5	IBM Security Access Manager Appliance 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 225081. **CVE ID : CVE-2022-22464**	https://www.ibm.com/support/pages/node/6601729, https://exchange.xforce.ibmcloud.com/vulnerabilities/225081	A-IBM-SECU-200722/239
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jul-2022	6.5	IBM Security Access Manager Appliance 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 225079. **CVE ID : CVE-2022-22463**	https://www.ibm.com/support/pages/node/6601729, https://exchange.xforce.ibmcloud.com/vulnerabilities/225079	A-IBM-SECU-200722/240
Affected Version(s): 10.0.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Jul-2022	7.8	IBM Security Access Manager Appliance 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 could allow a local user to obtain elevated privileges due to improper access permissions. IBM X-Force ID: 225082. **CVE ID : CVE-2022-22465**	https://www.ibm.com/support/pages/node/6601729, https://exchange.xforce.ibmcloud.com/vulnerabilities/225082	A-IBM-SECU-200722/241
Inadequate Encryption Strength	08-Jul-2022	7.5	IBM Security Access Manager Appliance 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 225081. **CVE ID : CVE-2022-22464**	https://www.ibm.com/support/pages/node/6601729, https://exchange.xforce.ibmcloud.com/vulnerabilities/225081	A-IBM-SECU-200722/242
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jul-2022	6.5	IBM Security Access Manager Appliance 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database.	https://www.ibm.com/support/pages/node/6601729, https://exchange.xforce.ibmcloud.com/vulnerabilities/225079	A-IBM-SECU-200722/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 225079. **CVE ID : CVE-2022-22463**		
Affected Version(s): 10.0.2.0					
N/A	08-Jul-2022	7.8	IBM Security Access Manager Appliance 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 could allow a local user to obtain elevated privileges due to improper access permissions. IBM X-Force ID: 225082. **CVE ID : CVE-2022-22465**	https://www.ibm.com/support/pages/node/6601729, https://exchange.xforce.ibmcloud.com/vulnerabilities/225082	A-IBM-SECU-200722/244
Inadequate Encryption Strength	08-Jul-2022	7.5	IBM Security Access Manager Appliance 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 225081. **CVE ID : CVE-2022-22464**	https://www.ibm.com/support/pages/node/6601729, https://exchange.xforce.ibmcloud.com/vulnerabilities/225081	A-IBM-SECU-200722/245
Improper Neutralization of Special Elements used in an SQL Command	08-Jul-2022	6.5	IBM Security Access Manager Appliance 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which	https://www.ibm.com/support/pages/node/6601729, https://exchange.xforce.ibmcloud.com/vulne	A-IBM-SECU-200722/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 225079. **CVE ID : CVE-2022-22463**	rabilities/225079	
Affected Version(s): 10.0.3.0					
N/A	08-Jul-2022	7.8	IBM Security Access Manager Appliance 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 could allow a local user to obtain elevated privileges due to improper access permissions. IBM X-Force ID: 225082. **CVE ID : CVE-2022-22465**	https://www.ibm.com/support/pages/node/6601729, https://exchange.xforce.ibmcloud.com/vulnerabilities/225082	A-IBM-SECU-200722/247
Inadequate Encryption Strength	08-Jul-2022	7.5	IBM Security Access Manager Appliance 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 225081. **CVE ID : CVE-2022-22464**	https://www.ibm.com/support/pages/node/6601729, https://exchange.xforce.ibmcloud.com/vulnerabilities/225081	A-IBM-SECU-200722/248
Improper Neutralization of Special	08-Jul-2022	6.5	IBM Security Access Manager Appliance 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0	https://www.ibm.com/support/pages/node/6601729,	A-IBM-SECU-200722/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 225079. **CVE ID : CVE-2022-22463**	https://exchange.xforce.ibmcloud.com/vulnerabilities/225079	
Product: urbancode_deploy					
Affected Version(s): 7.0.5.10					
Cleartext Storage of Sensitive Information	01-Jul-2022	5.5	IBM UrbanCode Deploy (UCD) 6.2.7.15, 7.0.5.10, 7.1.2.6, and 7.2.2.1 could disclose sensitive database information to a local user in plain text. IBM X-Force ID: 221008. **CVE ID : CVE-2022-22367**	https://www.ibm.com/support/pages/node/6600067, https://exchange.xforce.ibmcloud.com/vulnerabilities/221008	A-IBM-URBA-200722/250
Cleartext Storage of Sensitive Information	01-Jul-2022	4.4	IBM UrbanCode Deploy (UCD) 6.2.7.15, 7.0.5.10, 7.1.2.6, and 7.2.2.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 22106. **CVE ID : CVE-2022-22366**	https://www.ibm.com/support/pages/node/6600065, https://exchange.xforce.ibmcloud.com/vulnerabilities/221006	A-IBM-URBA-200722/251
Affected Version(s): 7.1.2.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	01-Jul-2022	5.5	IBM UrbanCode Deploy (UCD) 6.2.7.15, 7.0.5.10, 7.1.2.6, and 7.2.2.1 could disclose sensitive database information to a local user in plain text. IBM X-Force ID: 221008. **CVE ID : CVE-2022-22367**	https://www.ibm.com/support/pages/node/6600067, https://exchange.xforce.ibmcloud.com/vulnerabilities/221008	A-IBM-URBA-200722/252
Cleartext Storage of Sensitive Information	01-Jul-2022	4.4	IBM UrbanCode Deploy (UCD) 6.2.7.15, 7.0.5.10, 7.1.2.6, and 7.2.2.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 22106. **CVE ID : CVE-2022-22366**	https://www.ibm.com/support/pages/node/6600065, https://exchange.xforce.ibmcloud.com/vulnerabilities/221006	A-IBM-URBA-200722/253
Affected Version(s): 7.2.2.1					
Cleartext Storage of Sensitive Information	01-Jul-2022	5.5	IBM UrbanCode Deploy (UCD) 6.2.7.15, 7.0.5.10, 7.1.2.6, and 7.2.2.1 could disclose sensitive database information to a local user in plain text. IBM X-Force ID: 221008. **CVE ID : CVE-2022-22367**	https://www.ibm.com/support/pages/node/6600067, https://exchange.xforce.ibmcloud.com/vulnerabilities/221008	A-IBM-URBA-200722/254
Cleartext Storage of Sensitive Information	01-Jul-2022	4.4	IBM UrbanCode Deploy (UCD) 6.2.7.15, 7.0.5.10, 7.1.2.6, and 7.2.2.1 stores user credentials in plain clear text which can	https://www.ibm.com/support/pages/node/6600065, https://exchange.xforce.ibmcloud.com/vulne	A-IBM-URBA-200722/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be read by a local user. IBM X-Force ID: 22106. **CVE ID : CVE-2022-22366**	rabilities/221006	
Affected Version(s): 6.2.7.15					
Cleartext Storage of Sensitive Information	01-Jul-2022	5.5	IBM UrbanCode Deploy (UCD) 6.2.7.15, 7.0.5.10, 7.1.2.6, and 7.2.2.1 could disclose sensitive database information to a local user in plain text. IBM X-Force ID: 221008. **CVE ID : CVE-2022-22367**	https://www.ibm.com/support/pages/node/6600067, https://exchange.xforce.ibmcloud.com/vulnerabilities/221008	A-IBM-URBA-200722/256
Cleartext Storage of Sensitive Information	01-Jul-2022	4.4	IBM UrbanCode Deploy (UCD) 6.2.7.15, 7.0.5.10, 7.1.2.6, and 7.2.2.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 22106. **CVE ID : CVE-2022-22366**	https://www.ibm.com/support/pages/node/6600065, https://exchange.xforce.ibmcloud.com/vulnerabilities/221006	A-IBM-URBA-200722/257
Product: websphere_application_server					
Affected Version(s): From (including) 17.0.0.3 Up to (excluding) 22.0.0.8					
Authentication Bypass by Spoofing	08-Jul-2022	8.8	IBM WebSphere Application Server Liberty 17.0.0.3 through 22.0.0.7 and Open Liberty are vulnerable to identity spoofing by an authenticated user using a specially	https://www.ibm.com/support/pages/node/6602015, https://exchange.xforce.ibmcloud.com/vulnerabilities/225604	A-IBM-WEBS-200722/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted request. IBM X-Force ID: 225604. **CVE ID : CVE-2022-22476**		
Vendor: idayrus					
Product: e-voting					
Affected Version(s): * Up to (excluding) 2022-05-08					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The idayrus/evoting repository before 2022-05-08 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31508**	https://github.com/idayrus/evoting/commit/241d92a4d68f524365a6322b5bbcfaa7d9abc8a3	A-IDA-E-VO-200722/259
Vendor: iedadata					
Product: usap-dc_web_submission_and_dataset_search					
Affected Version(s): * Up to (including) 1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The iedadata/usap-dc-website repository through 1.0.1 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31509**	N/A	A-IED-USAP-200722/260
Vendor: ingredient_stock_management_system_project					
Product: ingredient_stock_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special	05-Jul-2022	9.8	An access control issue in Ingredient Stock Management System v1.0 allows	N/A	A-ING-INGR-200722/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			attackers to take over user accounts via a crafted POST request to /isms/classes/Users.php. **CVE ID : CVE-2022-32310**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2022	9.8	Ingredient Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /isms/admin/stocks/view_stock.php. **CVE ID : CVE-2022-32311**	N/A	A-ING-INGR-200722/262
Vendor: internshipsystem_project					
Product: internshipsystem					
Affected Version(s): * Up to (including) 2018-05-22					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The waveyan/internshipsystem repository through 2018-05-22 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31562**	N/A	A-INT-INTE-200722/263
Vendor: Iobit					
Product: advanced_systemcare					
Affected Version(s): 15					
Files or Directories Accessible	06-Jul-2022	7.8	IOBit Advanced System Care (Asc.exe) 15 and Action	http://iobit.com	A-IOB-ADVA-200722/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to External Parties			Download Center both download components of IOBit suite into ProgramData folder, ProgramData folder has "rwx" permissions for unprivileged users. Low privilege users can use SetOpLock to wait for CreateProcess and switch the genuine component with a malicious executable thus gaining code execution as a high privilege user (Low Privilege -> high integrity ADMIN). **CVE ID : CVE-2022-24138**		
Product: advanced_system_care					
Affected Version(s): 15					
Exposure of Resource to Wrong Sphere	06-Jul-2022	7.8	In IOBit Advanced System Care (AscService.exe) 15, an attacker with SEImpersonatePrivilege can create a named pipe with the same name as one of ASCService's named pipes. ASCService first tries to connect before trying to create the named pipes, because of that during login the service will try to connect to the attacker which will	http://iobit.com	A-IOB-ADVA-200722/265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to either escalation of privileges (through token manipulation and ImpersonateNamedPipeClient()) from ADMIN -> SYSTEM or from Local ADMIN-> Domain ADMIN depending on the user and named pipe that is used. **CVE ID : CVE-2022-24139**		
Download of Code Without Integrity Check	06-Jul-2022	6.6	IOBit Advanced System Care 15, iTop Screen Recorder 2.1, iTop VPN 3.2, Driver Booster 9, and iTop Screenshot sends HTTP requests in their update procedure in order to download a config file. After downloading the config file, the products will parse the HTTP location of the update from the file and will try to install the update automatically with ADMIN privileges. An attacker Intercepting this communication can supply the product a fake config file with malicious locations for the updates thus gaining a remote code	http://iobit.com	A-IOB-ADVA-200722/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution on an endpoint. **CVE ID : CVE-2022-24140**		
Product: driver_booster					
Affected Version(s): 9					
Download of Code Without Integrity Check	06-Jul-2022	6.6	IOBit Advanced System Care 15, iTop Screen Recorder 2.1, iTop VPN 3.2, Driver Booster 9, and iTop Screenshot sends HTTP requests in their update procedure in order to download a config file. After downloading the config file, the products will parse the HTTP location of the update from the file and will try to install the update automatically with ADMIN privileges. An attacker Intercepting this communication can supply the product a fake config file with malicious locations for the updates thus gaining a remote code execution on an endpoint. **CVE ID : CVE-2022-24140**	http://iobit.com	A-IOB-DRIV-200722/267
Product: itop_screenshot					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Download of Code Without Integrity Check	06-Jul-2022	6.6	IOBit Advanced System Care 15, iTop Screen Recorder 2.1, iTop VPN 3.2, Driver Booster 9, and iTop Screenshot sends HTTP requests in their update procedure in order to download a config file. After downloading the config file, the products will parse the HTTP location of the update from the file and will try to install the update automatically with ADMIN privileges. An attacker Intercepting this communication can supply the product a fake config file with malicious locations for the updates thus gaining a remote code execution on an endpoint. **CVE ID : CVE-2022-24140**	http://iobit.com	A-IOB-ITOP-200722/268
Product: itop_screen_recorder					
Affected Version(s): 2.1					
Download of Code Without Integrity Check	06-Jul-2022	6.6	IOBit Advanced System Care 15, iTop Screen Recorder 2.1, iTop VPN 3.2, Driver Booster 9, and iTop Screenshot sends HTTP requests in their update procedure in order to	http://iobit.com	A-IOB-ITOP-200722/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			download a config file. After downloading the config file, the products will parse the HTTP location of the update from the file and will try to install the update automatically with ADMIN privileges. An attacker Intercepting this communication can supply the product a fake config file with malicious locations for the updates thus gaining a remote code execution on an endpoint. **CVE ID : CVE-2022-24140**		
Product: itop_vpn					
Affected Version(s): 3.2					
Download of Code Without Integrity Check	06-Jul-2022	6.6	IOBit Advanced System Care 15, iTop Screen Recorder 2.1, iTop VPN 3.2, Driver Booster 9, and iTop Screenshot sends HTTP requests in their update procedure in order to download a config file. After downloading the config file, the products will parse the HTTP location of the update from the file and will try to install the update	http://iobit.com	A-IOB-ITOP-200722/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automatically with ADMIN privileges. An attacker Intercepting this communication can supply the product a fake config file with malicious locations for the updates thus gaining a remote code execution on an endpoint. **CVE ID : CVE-2022-24140**		
N/A	06-Jul-2022	5.4	The iTopVPNmini.exe component of iTop VPN 3.2 will try to connect to datastate_iTopVPN_Pipe_Server on a loop. An attacker that opened a named pipe with the same name can use it to gain the token of another user by listening for connections and abusing ImpersonateNamedPipeClient(). **CVE ID : CVE-2022-24141**	http://iobit.com	A-IOB-ITOP-200722/271
Vendor: Jetbrains					
Product: hub					
Affected Version(s): * Up to (excluding) 2022.2.14799					
N/A	01-Jul-2022	5.3	In JetBrains Hub before 2022.2.14799, insufficient access control allowed the hijacking of untrusted services	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-HUB-200722/272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34894		
Vendor: joinbookwyrm					
Product: bookwyrm					
Affected Version(s): * Up to (excluding) 0.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2022	6.1	Bookwyrm is an open source social reading and reviewing program. Versions of Bookwyrm prior to 0.4.1 did not properly sanitize html being rendered to users. Unprivileged users are able to inject scripts into user profiles, book descriptions, and statuses. These vulnerabilities may be exploited as cross site scripting attacks on users viewing these fields. Users are advised to upgrade to version 0.4.1. There are no known workarounds for this issue. **CVE ID : CVE-2022-31136**	https://github.com/bookwyrm-social/bookwyrm/security/advisories/GHSA-2cfh-v7rf-pxfp, https://github.com/bookwyrm-social/bookwyrm/commit/fe33fdcf564a6a5667aef75d5456bea08feab50d	A-JOI-BOOK-200722/273
Vendor: jpegoptim_project					
Product: jpegoptim					
Affected Version(s): 1.4.7					
Out-of-bounds Read	01-Jul-2022	6.5	JPEGOPTIM v1.4.7 was discovered to contain a segmentation violation which is caused by a READ	N/A	A-JPE-JPEG-200722/274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory access at jpegoptim.c. **CVE ID : CVE-2022-32325**		
Vendor: jsrsasign_project					
Product: jsrsasign					
Affected Version(s): From (including) 4.8.0 Up to (excluding) 10.5.25					
Improper Verification of Cryptographic Signature	01-Jul-2022	9.8	The package jsrsasign before 10.5.25 are vulnerable to Improper Verification of Cryptographic Signature when JWS or JWT signature with non Base64URL encoding special characters or number escaped characters may be validated as valid by mistake. Workaround: Validate JWS or JWT signature if it has Base64URL and dot safe string before executing JWS.verify() or JWS.verifyJWT() method. **CVE ID : CVE-2022-25898**	https://github.com/kjur/jsrsasign/releases/tag/10.5.25, https://snyk.io/vuln/SNYK-JS-JSRSASIGN-2869122, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2935898, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2935896	A-JSR-JSRS-200722/275
Vendor: karaokey_project					
Product: karaokey					
Affected Version(s): * Up to (including) 2019-12-11					
Improper Limitation of a Pathname to a Restricted Directory	11-Jul-2022	9.3	The NotVinay/karaokey repository through 2019-12-11 on GitHub allows absolute path traversal because the Flask send_file	N/A	A-KAR-KARA-200722/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			function is used unsafely. **CVE ID : CVE-2022-31522**		
Vendor: kg-fashion-chatbot_project					
Product: kg-fashion-chatbot					
Affected Version(s): * Up to (including) 2018-05-22					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The yuriyouzhou/KG-fashion-chatbot repository through 2018-05-22 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31587**	N/A	A-KG--KG-F-200722/277
Vendor: kitestudio					
Product: core_plugin_for_kitestudio_themes					
Affected Version(s): * Up to (excluding) 2.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2022	6.1	The core plugin for kitestudio WordPress plugin before 2.3.1 does not sanitise and escape some parameters before outputting them back in a response of an AJAX action, available to both unauthenticated and authenticated users when a premium theme from the vendor is active, leading to a Reflected Cross-Site Scripting.	N/A	A-KIT-CORE-200722/278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1951		
Vendor: kotekan_project					
Product: kotekan					
Affected Version(s): * Up to (including) 2021.11					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The kotekan/kotekan repository through 2021.11 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31539**	N/A	A-KOT-KOTE-200722/279
Vendor: krypton_project					
Product: krypton					
Affected Version(s): * Up to (including) 2021-06-03					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The BolunHan/Krypton repository through 2021-06-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31513**	N/A	A-KRY-KRYP-200722/280
Vendor: libmobi_project					
Product: libmobi					
Affected Version(s): * Up to (excluding) 0.11					
NULL Pointer Dereference	01-Jul-2022	5.5	NULL Pointer Dereference in GitHub repository bfabiszewski/libmobi prior to 0.11.	https://huntr.dev/bounties/68c249e2-779d-4871-b7e3-851f03aca2de,	A-LIB-LIBM-200722/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2279	https://github.com/bfabiszewski/libmobi/commit/c0699c8693c47f14a2e57dec7292e862ac7adf9c	
Vendor: link-preview-js_project					
Product: link-preview-js					
Affected Version(s): * Up to (excluding) 2.1.16					
Server-Side Request Forgery (SSRF)	01-Jul-2022	5.5	The package link-preview-js before 2.1.16 are vulnerable to Server-side Request Forgery (SSRF) which allows attackers to send arbitrary requests to the local network and read the response. This is due to flawed DNS rebinding protection. **CVE ID : CVE-2022-25876**	https://github.com/ospfranco/link-preview-js/issues/115, https://github.com/ospfranco/link-preview-js/pull/117, https://snyk.io/vuln/SNYK-JS-LINKPREVIEWJS-2933520	A-LIN-LINK-200722/282
Vendor: Linuxfoundation					
Product: kubeedge					
Affected Version(s): * Up to (excluding) 1.9.4					
Uncontrolled Resource Consumption	11-Jul-2022	7.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, the ServiceBus server on the edge side may be susceptible to a DoS	https://github.com/kubeedge/kubeedge/pull/4042, https://github.com/kubeedge/kubeedge/security/advisories/GHSA-vwm6-qc77-v2rh, https://github.com/kubeedge	A-LIN-KUBE-200722/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack if an HTTP request containing a very large Body is sent to it. It is possible for the node to be exhausted of memory. The consequence of the exhaustion is that other services on the node, e.g. other containers, will be unable to allocate memory and thus causing a denial of service. Malicious apps accidentally pulled by users on the host and have the access to send HTTP requests to localhost may make an attack. It will be affected only when users enable the `ServiceBus` module in the config file `edgecore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable the `ServiceBus` module in the config file `edgecore.yaml`. **CVE ID : CVE-2022-31073**	/kubeedge/pull/4039, https://github.com/kubeedge/kubeedge/pull/4038	
Uncontrolled Resource Consumption	11-Jul-2022	6.5	KubeEdge is an open source system for extending native containerized application orchestration	https://github.com/kubeedge/kubeedge/security/advisories/GHSA-w52j-3457-q9wr	A-LIN-KUBE-200722/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, several endpoints in the Cloud AdmissionController may be susceptible to a DoS attack if an HTTP request containing a very large Body is sent to it. The consequence of the exhaustion is that the Cloud AdmissionController will be in denial of service. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. There is currently no known workaround. **CVE ID : CVE-2022-31074**		
Uncontrolled Resource Consumption	11-Jul-2022	6.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, EdgeCore may be susceptible to a DoS attack on CloudHub if an attacker was to send a well-crafted HTTP request to `/edge.crt`. If an attacker can send a	https://github.com/kubeedge/kubeedge/security/advisories/GHSA-x3px-2p95-f6jr	A-LIN-KUBE-200722/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			well-crafted HTTP request to CloudHub, and that request has a very large body, that request can crash the HTTP service through a memory exhaustion vector. The request body is being read into memory, and a body that is larger than the available memory can lead to a successful attack. Because the request would have to make it through authorization, only authorized users may perform this attack. The consequence of the exhaustion is that CloudHub will be in denial of service. KubeEdge is affected only when users enable the CloudHub module in the file `cloudcore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable the CloudHub switch in the config file `cloudcore.yaml`. **CVE ID : CVE-2022-31075**		
Uncontrolled Resource Consumption	11-Jul-2022	6.5	KubeEdge is an open source system for extending native containerized application	https://github.com/kubeedge/kubeedge/security/advisorie	A-LIN-KUBE-200722/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, the CloudCore Router does not impose a limit on the size of responses to requests made by the REST handler. An attacker could use this weakness to make a request that will return an HTTP response with a large body and cause DoS of CloudCore. In the HTTP Handler API, the rest handler makes a request to a pre-specified handle. The handle will return an HTTP response that is then read into memory. The consequence of the exhaustion is that CloudCore will be in a denial of service. Only an authenticated user of the cloud can make an attack. It will be affected only when users enable `router` module in the config file `cloudcore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable the router switch in	s/GHSA-qpx3-9565-5xwm	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the config file `cloudcore.yaml`. **CVE ID : CVE-2022-31078**		
Uncontrolled Resource Consumption	11-Jul-2022	6.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, the Cloud Stream server and the Edge Stream server reads the entire message into memory without imposing a limit on the size of this message. An attacker can exploit this by sending a large message to exhaust memory and cause a DoS. The Cloud Stream server and the Edge Stream server are under DoS attack in this case. The consequence of the exhaustion is that the CloudCore and EdgeCore will be in a denial of service. Only an authenticated user can cause this issue. It will be affected only when users enable `cloudStream` module in the config file `cloudcore.yaml` and	https://github.com/kubeedge/kubeedge/security/advisories/GHSA-wrcr-x4qj-j543	A-LIN-KUBE-200722/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enable `edgeStream` module in the config file `edgecore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable cloudStream module in the config file `cloudcore.yaml` and disable edgeStream module in the config file `edgecore.yaml`. **CVE ID : CVE-2022-31079**		
Uncontrolled Resource Consumption	11-Jul-2022	6.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, a large response received by the viaduct WSClient can cause a DoS from memory exhaustion. The entire body of the response is being read into memory which could allow an attacker to send a request that returns a response with a large body. The consequence of the exhaustion is that the process which invokes a WSClient	https://github.com/kubeedge/kubeedge/security/advisories/GHSA-6wvc-6pww-qr4r	A-LIN-KUBE-200722/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will be in a denial of service. The software is affected If users who are authenticated to the edge side connect to `cloudhub` from the edge side through WebSocket protocol. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. There are currently no known workarounds. **CVE ID : CVE-2022-31080**		
Affected Version(s): From (including) 1.10.0 Up to (excluding) 1.10.2					
Uncontrolled Resource Consumption	11-Jul-2022	7.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, the ServiceBus server on the edge side may be susceptible to a DoS attack if an HTTP request containing a very large Body is sent to it. It is possible for the node to be exhausted of memory. The consequence of the exhaustion is that other services on the node, e.g. other containers, will be	https://github.com/kubeedge/kubeedge/pull/4042, https://github.com/kubeedge/kubeedge/security/advisories/GHSA-vwm6-qc77-v2rh, https://github.com/kubeedge/kubeedge/pull/4039, https://github.com/kubeedge/kubeedge/pull/4038	A-LIN-KUBE-200722/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unable to allocate memory and thus causing a denial of service. Malicious apps accidentally pulled by users on the host and have the access to send HTTP requests to localhost may make an attack. It will be affected only when users enable the `ServiceBus` module in the config file `edgecore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable the `ServiceBus` module in the config file `edgecore.yaml`. **CVE ID : CVE-2022-31073**		
Uncontrolled Resource Consumption	11-Jul-2022	6.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, several endpoints in the Cloud AdmissionController may be susceptible to a DoS attack if an HTTP request containing a very large Body is sent to	https://github.com/kubeedge/kubeedge/security/advisories/GHSA-w52j-3457-q9wr	A-LIN-KUBE-200722/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it. The consequence of the exhaustion is that the Cloud AdmissionController will be in denial of service. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. There is currently no known workaround. **CVE ID : CVE-2022-31074**		
Uncontrolled Resource Consumption	11-Jul-2022	6.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, EdgeCore may be susceptible to a DoS attack on CloudHub if an attacker was to send a well-crafted HTTP request to `/edge.crt`. If an attacker can send a well-crafted HTTP request to CloudHub, and that request has a very large body, that request can crash the HTTP service through a memory exhaustion vector. The request body is being read into memory, and a body that is larger than the available	https://github.com/kubeedge/kubeedge/security/advisories/GHSA-x3px-2p95-f6jr	A-LIN-KUBE-200722/291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory can lead to a successful attack. Because the request would have to make it through authorization, only authorized users may perform this attack. The consequence of the exhaustion is that CloudHub will be in denial of service. KubeEdge is affected only when users enable the CloudHub module in the file `cloudcore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable the CloudHub switch in the config file `cloudcore.yaml`. **CVE ID : CVE-2022-31075**		
Uncontrolled Resource Consumption	11-Jul-2022	6.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, the CloudCore Router does not impose a limit on the size of responses to requests made by the REST handler. An attacker could use this	https://github.com/kubeedge/kubeedge/security/advisories/GHSA-qpx3-9565-5xwm	A-LIN-KUBE-200722/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			weakness to make a request that will return an HTTP response with a large body and cause DoS of CloudCore. In the HTTP Handler API, the rest handler makes a request to a pre-specified handle. The handle will return an HTTP response that is then read into memory. The consequence of the exhaustion is that CloudCore will be in a denial of service. Only an authenticated user of the cloud can make an attack. It will be affected only when users enable `router` module in the config file `cloudcore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable the router switch in the config file `cloudcore.yaml`. **CVE ID : CVE-2022-31078**		
Uncontrolled Resource Consumption	11-Jul-2022	6.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to	https://github.com/kubeedge/kubeedge/security/advisories/GHSA-wrcr-x4qj-j543	A-LIN-KUBE-200722/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 1.11.1, 1.10.2, and 1.9.4, the Cloud Stream server and the Edge Stream server reads the entire message into memory without imposing a limit on the size of this message. An attacker can exploit this by sending a large message to exhaust memory and cause a DoS. The Cloud Stream server and the Edge Stream server are under DoS attack in this case. The consequence of the exhaustion is that the CloudCore and EdgeCore will be in a denial of service. Only an authenticated user can cause this issue. It will be affected only when users enable `cloudStream` module in the config file `cloudcore.yaml` and enable `edgeStream` module in the config file `edgecore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable cloudStream module in the config file `cloudcore.yaml` and disable edgeStream		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module in the config file `edgecore.yaml`. **CVE ID : CVE-2022-31079**		
Uncontrolled Resource Consumption	11-Jul-2022	6.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, a large response received by the viaduct WSClient can cause a DoS from memory exhaustion. The entire body of the response is being read into memory which could allow an attacker to send a request that returns a response with a large body. The consequence of the exhaustion is that the process which invokes a WSClient will be in a denial of service. The software is affected If users who are authenticated to the edge side connect to `cloudhub` from the edge side through WebSocket protocol. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and	https://github.com/kubeedge/kubeedge/security/advisories/GHSA-6wvc-6pww-qr4r	A-LIN-KUBE-200722/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.9.4. There are currently no known workarounds. **CVE ID : CVE-2022-31080**		
Affected Version(s): From (including) 1.11.0 Up to (excluding) 1.11.1					
Uncontrolled Resource Consumption	11-Jul-2022	7.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, the ServiceBus server on the edge side may be susceptible to a DoS attack if an HTTP request containing a very large Body is sent to it. It is possible for the node to be exhausted of memory. The consequence of the exhaustion is that other services on the node, e.g. other containers, will be unable to allocate memory and thus causing a denial of service. Malicious apps accidentally pulled by users on the host and have the access to send HTTP requests to localhost may make an attack. It will be affected only when users enable	https://github.com/kubeedge/kubeedge/pull/4042, https://github.com/kubeedge/kubeedge/security/advisories/GHSA-vwm6-qc77-v2rh, https://github.com/kubeedge/kubeedge/pull/4039, https://github.com/kubeedge/kubeedge/pull/4038	A-LIN-KUBE-200722/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the `ServiceBus` module in the config file `edgecore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable the `ServiceBus` module in the config file `edgecore.yaml`. **CVE ID : CVE-2022-31073**		
Uncontrolled Resource Consumption	11-Jul-2022	6.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, several endpoints in the Cloud AdmissionController may be susceptible to a DoS attack if an HTTP request containing a very large Body is sent to it. The consequence of the exhaustion is that the Cloud AdmissionController will be in denial of service. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. There is currently no known workaround.	https://github.com/kubeedge/kubeedge/security/advisories/GHSA-w52j-3457-q9wr	A-LIN-KUBE-200722/296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31074		
Uncontrolled Resource Consumption	11-Jul-2022	6.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, EdgeCore may be susceptible to a DoS attack on CloudHub if an attacker was to send a well-crafted HTTP request to `/edge.crt`. If an attacker can send a well-crafted HTTP request to CloudHub, and that request has a very large body, that request can crash the HTTP service through a memory exhaustion vector. The request body is being read into memory, and a body that is larger than the available memory can lead to a successful attack. Because the request would have to make it through authorization, only authorized users may perform this attack. The consequence of the exhaustion is that CloudHub will be in denial of service.	https://github.com/kubeedge/kubeedge/security/advisories/GHSA-x3px-2p95-f6jr	A-LIN-KUBE-200722/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			KubeEdge is affected only when users enable the CloudHub module in the file `cloudcore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable the CloudHub switch in the config file `cloudcore.yaml`. **CVE ID : CVE-2022-31075**		
Uncontrolled Resource Consumption	11-Jul-2022	6.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, the CloudCore Router does not impose a limit on the size of responses to requests made by the REST handler. An attacker could use this weakness to make a request that will return an HTTP response with a large body and cause DoS of CloudCore. In the HTTP Handler API, the rest handler makes a request to a pre-specified handle. The handle will return an HTTP	https://github.com/kubeedge/kubeedge/security/advisories/GHSA-qpx3-9565-5xwm	A-LIN-KUBE-200722/298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response that is then read into memory. The consequence of the exhaustion is that CloudCore will be in a denial of service. Only an authenticated user of the cloud can make an attack. It will be affected only when users enable `router` module in the config file `cloudcore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable the router switch in the config file `cloudcore.yaml`. **CVE ID : CVE-2022-31078**		
Uncontrolled Resource Consumption	11-Jul-2022	6.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to versions 1.11.1, 1.10.2, and 1.9.4, the Cloud Stream server and the Edge Stream server reads the entire message into memory without imposing a limit on the size of this message. An attacker can exploit this by sending a large	https://github.com/kubeedge/kubeedge/security/advisories/GHSA-wrcr-x4qj-j543	A-LIN-KUBE-200722/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message to exhaust memory and cause a DoS. The Cloud Stream server and the Edge Stream server are under DoS attack in this case. The consequence of the exhaustion is that the CloudCore and EdgeCore will be in a denial of service. Only an authenticated user can cause this issue. It will be affected only when users enable `cloudStream` module in the config file `cloudcore.yaml` and enable `edgeStream` module in the config file `edgecore.yaml`. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. As a workaround, disable cloudStream module in the config file `cloudcore.yaml` and disable edgeStream module in the config file `edgecore.yaml`. **CVE ID : CVE-2022-31079**		
Uncontrolled Resource Consumption	11-Jul-2022	6.5	KubeEdge is an open source system for extending native containerized application orchestration capabilities to hosts at Edge. Prior to	https://github.com/kubeedge/kubeedge/security/advisories/GHSA-6wvc-6pww-qr4r	A-LIN-KUBE-200722/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 1.11.1, 1.10.2, and 1.9.4, a large response received by the viaduct WSClient can cause a DoS from memory exhaustion. The entire body of the response is being read into memory which could allow an attacker to send a request that returns a response with a large body. The consequence of the exhaustion is that the process which invokes a WSClient will be in a denial of service. The software is affected If users who are authenticated to the edge side connect to `cloudhub` from the edge side through WebSocket protocol. This bug has been fixed in Kubeedge 1.11.1, 1.10.2, and 1.9.4. There are currently no known workarounds. **CVE ID : CVE-2022-31080**		
Vendor: Litecart					
Product: litecart					
Affected Version(s): * Up to (excluding) 2.4.2					
Improper Neutralization of	11-Jul-2022	6.1	Cross-site scripting vulnerability in LiteCart versions	https://github.com/litecart/litecart/commit	A-LIT-LITE-200722/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			prior to 2.4.2 allows a remote attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2022-27168**	/050fea86cc162f3da2f7824f586602125a0f6d63, https://jvn.jp/en/jp/JVN32625020/index.html	
Vendor: livro_python_project					
Product: livro_python					
Affected Version(s): * Up to (including) 2018-06-06					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The duducosmos/livro_python repository through 2018-06-06 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31575**	N/A	A-LIV-LIVR-200722/302
Vendor: logstash-management-api_project					
Product: logstash-management-api					
Affected Version(s): * Up to (including) 2020-05-04					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The Luxas98/logstash-management-api repository through 2020-05-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31520**	N/A	A-LOG-LOGS-200722/303
Vendor: LUA					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: lua					
Affected Version(s): * Up to (including) 5.4.4					
Out-of-bounds Write	01-Jul-2022	7.5	An issue in the component luaG_runerror of Lua v5.4.4 and below leads to a heap-buffer overflow when a recursive error occurs. **CVE ID : CVE-2022-33099**	https://lua-users.org/lists/lua-l/2022-05/msg00073.html, https://lua-users.org/lists/lua-l/2022-05/msg00042.html, https://lua-users.org/lists/lua-l/2022-05/msg00035.html, https://github.com/lua/lua/commit/42d40581dd919fb134c07027ca1ce0844c670daf	A-LUA-LUA-200722/304
Vendor: Lxml					
Product: lxml					
Affected Version(s): * Up to (excluding) 4.9.1					
NULL Pointer Dereference	05-Jul-2022	7.5	NULL Pointer Dereference allows attackers to cause a denial of service (or application crash). This only applies when lxml is used together with libxml2 2.9.10 through 2.9.14. libxml2 2.9.9 and earlier are not affected. It allows triggering crashes through forged input data, given a vulnerable code	https://huntr.dev/bounties/8264e74f-edda-4c40-9956-49de635105ba, https://github.com/lxml/lxml/commit/86368e9cf70a0ad23cccd5ee32de847149af0c6f	A-LXM-LXML-200722/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sequence in the application. The vulnerability is caused by the iterwalk function (also used by the canonicalize function). Such code shouldn't be in wide-spread use, given that parsing + iterwalk would usually be replaced with the more efficient iterparse function. However, an XML converter that serialises to C14N would also be vulnerable, for example, and there are legitimate use cases for this code sequence. If untrusted input is received (also remotely) and processed via iterwalk function, a crash can be triggered. **CVE ID : CVE-2022-2309**		
Vendor: Magnolia-cms					
Product: magnolia_cms					
Affected Version(s): 6.2.19					
Improper Neutralization of Input During Web Page Generation	07-Jul-2022	6.1	Magnolia CMS v6.2.19 was discovered to contain a cross-site scripting (XSS) vulnerability via the Edit Contact function. This vulnerability	N/A	A-MAG-MAGN-200722/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2022-33098**		
Vendor: Mariadb					
Product: mariadb					
Affected Version(s): 10.9.0					
Reachable Assertion	01-Jul-2022	7.5	MariaDB v10.5 to v10.7 was discovered to contain an assertion failure at table->get_ref_count() == 0 in dict0dict.cc. **CVE ID : CVE-2022-32082**	N/A	A-MAR-MARI-200722/307
Affected Version(s): From (including) 10.2.0 Up to (excluding) 10.2.44					
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.6.1 was discovered to contain a segmentation fault via the component Item_subselect::init_expr_cache_tracker. **CVE ID : CVE-2022-32083**	N/A	A-MAR-MARI-200722/308
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component sub_select. **CVE ID : CVE-2022-32084**	N/A	A-MAR-MARI-200722/309
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component	N/A	A-MAR-MARI-200722/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Item_func_in::cleanup /Item::cleanup_processor. **CVE ID : CVE-2022-32085**		
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Exec_time_tracker::get_loops/Filesort_tracker::report_use/filesort. **CVE ID : CVE-2022-32088**	N/A	A-MAR-MARI-200722/311
Affected Version(s): From (including) 10.3.0 Up to (excluding) 10.3.35					
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.6.1 was discovered to contain a segmentation fault via the component Item_subselect::init_expr_cache_tracker. **CVE ID : CVE-2022-32083**	N/A	A-MAR-MARI-200722/312
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component sub_select. **CVE ID : CVE-2022-32084**	N/A	A-MAR-MARI-200722/313
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Item_func_in::cleanup	N/A	A-MAR-MARI-200722/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/Item::cleanup_processor. **CVE ID : CVE-2022-32085**		
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Item_args::walk_args. **CVE ID : CVE-2022-32087**	N/A	A-MAR-MARI-200722/315
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Exec_time_tracker::get_loops/Filesort_tracker::report_use/filesort. **CVE ID : CVE-2022-32088**	N/A	A-MAR-MARI-200722/316
Affected Version(s): From (including) 10.4.0 Up to (excluding) 10.4.25					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2022	9.8	MariaDB v10.4 to v10.7 was discovered to contain an use-after-poison in prepare_inplace_add_virtual at /storage/innobase/handler/handler0alter.cc. **CVE ID : CVE-2022-32081**	N/A	A-MAR-MARI-200722/317
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.6.1 was discovered to contain a segmentation fault via the component	N/A	A-MAR-MARI-200722/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Item_subselect::init_expr_cache_tracker. **CVE ID : CVE-2022-32083**		
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component sub_select. **CVE ID : CVE-2022-32084**	N/A	A-MAR-MARI-200722/319
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Item_func_in::cleanup /Item::cleanup_processor. **CVE ID : CVE-2022-32085**	N/A	A-MAR-MARI-200722/320
N/A	01-Jul-2022	7.5	MariaDB v10.4 to v10.8 was discovered to contain a segmentation fault via the component Item_field::fix_outer_field. **CVE ID : CVE-2022-32086**	N/A	A-MAR-MARI-200722/321
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Item_args::walk_args. **CVE ID : CVE-2022-32087**	N/A	A-MAR-MARI-200722/322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Exec_time_tracker::get_loops/Filesort_tracker::report_use/filesort. **CVE ID : CVE-2022-32088**	N/A	A-MAR-MARI-200722/323
Affected Version(s): From (including) 10.5.0 Up to (excluding) 10.5.16					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2022	9.8	MariaDB v10.4 to v10.7 was discovered to contain an use-after-poison in prepare_inplace_add_virtual at /storage/innobase/handler/handler0alter.cc. **CVE ID : CVE-2022-32081**	N/A	A-MAR-MARI-200722/324
Reachable Assertion	01-Jul-2022	7.5	MariaDB v10.5 to v10.7 was discovered to contain an assertion failure at table->get_ref_count() == 0 in dict0dict.cc. **CVE ID : CVE-2022-32082**	N/A	A-MAR-MARI-200722/325
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.6.1 was discovered to contain a segmentation fault via the component Item_subselect::init_expr_cache_tracker. **CVE ID : CVE-2022-32083**	N/A	A-MAR-MARI-200722/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component sub_select. **CVE ID : CVE-2022-32084**	N/A	A-MAR-MARI-200722/327
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Item_func_in::cleanup /Item::cleanup_processor. **CVE ID : CVE-2022-32085**	N/A	A-MAR-MARI-200722/328
N/A	01-Jul-2022	7.5	MariaDB v10.4 to v10.8 was discovered to contain a segmentation fault via the component Item_field::fix_outer_field. **CVE ID : CVE-2022-32086**	N/A	A-MAR-MARI-200722/329
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Item_args::walk_args. **CVE ID : CVE-2022-32087**	N/A	A-MAR-MARI-200722/330
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Exec_time_tracker::ge	N/A	A-MAR-MARI-200722/331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			t_loops/Filesort_tracker::report_use/filesort. **CVE ID : CVE-2022-32088**		
N/A	01-Jul-2022	7.5	MariaDB v10.5 to v10.7 was discovered to contain a segmentation fault via the component st_select_lex_unit::exclude_level. **CVE ID : CVE-2022-32089**	N/A	A-MAR-MARI-200722/332
Affected Version(s): From (including) 10.6.0 Up to (excluding) 10.6.8					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2022	9.8	MariaDB v10.4 to v10.7 was discovered to contain an use-after-poison in prepare_inplace_add_virtual at /storage/innobase/handler/handler0alter.cc. **CVE ID : CVE-2022-32081**	N/A	A-MAR-MARI-200722/333
Reachable Assertion	01-Jul-2022	7.5	MariaDB v10.5 to v10.7 was discovered to contain an assertion failure at table->get_ref_count() == 0 in dict0dict.cc. **CVE ID : CVE-2022-32082**	N/A	A-MAR-MARI-200722/334
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.6.1 was discovered to contain a segmentation fault via the component Item_subselect::init_expr_cache_tracker.	N/A	A-MAR-MARI-200722/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32083		
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component sub_select. **CVE ID : CVE-2022-32084**	N/A	A-MAR-MARI-200722/336
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Item_func_in::cleanup /Item::cleanup_processor. **CVE ID : CVE-2022-32085**	N/A	A-MAR-MARI-200722/337
N/A	01-Jul-2022	7.5	MariaDB v10.4 to v10.8 was discovered to contain a segmentation fault via the component Item_field::fix_outer_field. **CVE ID : CVE-2022-32086**	N/A	A-MAR-MARI-200722/338
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Item_args::walk_args. **CVE ID : CVE-2022-32087**	N/A	A-MAR-MARI-200722/339
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via	N/A	A-MAR-MARI-200722/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the component Exec_time_tracker::get_loops/Filesort_tracker::report_use/filesort. **CVE ID : CVE-2022-32088**		
N/A	01-Jul-2022	7.5	MariaDB v10.5 to v10.7 was discovered to contain a segmentation fault via the component st_select_lex_unit::exclude_level. **CVE ID : CVE-2022-32089**	N/A	A-MAR-MARI-200722/341
Affected Version(s): From (including) 10.7.0 Up to (excluding) 10.7.4					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2022	9.8	MariaDB v10.4 to v10.7 was discovered to contain an use-after-poison in prepare_inplace_add_virtual at /storage/innobase/handler/handler0alter.cc. **CVE ID : CVE-2022-32081**	N/A	A-MAR-MARI-200722/342
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2022	9.8	MariaDB v10.7 was discovered to contain an use-after-poison in in __interceptor_memset at /libsanitizer/sanitizer_common/sanitizer_common_interceptors.inc. **CVE ID : CVE-2022-32091**	N/A	A-MAR-MARI-200722/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	01-Jul-2022	7.5	MariaDB v10.5 to v10.7 was discovered to contain an assertion failure at table->get_ref_count() == 0 in dict0dict.cc. **CVE ID : CVE-2022-32082**	N/A	A-MAR-MARI-200722/344
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.6.1 was discovered to contain a segmentation fault via the component Item_subselect::init_expr_cache_tracker. **CVE ID : CVE-2022-32083**	N/A	A-MAR-MARI-200722/345
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component sub_select. **CVE ID : CVE-2022-32084**	N/A	A-MAR-MARI-200722/346
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Item_func_in::cleanup /Item::cleanup_processor. **CVE ID : CVE-2022-32085**	N/A	A-MAR-MARI-200722/347
N/A	01-Jul-2022	7.5	MariaDB v10.4 to v10.8 was discovered to contain a segmentation fault via the component	N/A	A-MAR-MARI-200722/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Item_field::fix_outer_field. **CVE ID : CVE-2022-32086**		
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Item_args::walk_args. **CVE ID : CVE-2022-32087**	N/A	A-MAR-MARI-200722/349
N/A	01-Jul-2022	7.5	MariaDB v10.2 to v10.7 was discovered to contain a segmentation fault via the component Exec_time_tracker::get_loops/Filesort_tracker::report_use/filesort. **CVE ID : CVE-2022-32088**	N/A	A-MAR-MARI-200722/350
N/A	01-Jul-2022	7.5	MariaDB v10.5 to v10.7 was discovered to contain a segmentation fault via the component st_select_lex_unit::exclude_level. **CVE ID : CVE-2022-32089**	N/A	A-MAR-MARI-200722/351
Affected Version(s): From (including) 10.8.0 Up to (excluding) 10.8.3					
Reachable Assertion	01-Jul-2022	7.5	MariaDB v10.5 to v10.7 was discovered to contain an assertion failure at table->get_ref_count() == 0 in dict0dict.cc.	N/A	A-MAR-MARI-200722/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32082		
Vendor: Maxfoundry					
Product: wp-paginate					
Affected Version(s): * Up to (excluding) 2.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2022	4.8	The WP-Paginate WordPress plugin before 2.1.9 does not escape one of its settings, which could allow high privilege users to perform Stored Cross-Site Scripting attacks when unfiltered_html is disallowed **CVE ID : CVE-2022-2050**	N/A	A-MAX-WP-P-200722/353
Vendor: md2roff_project					
Product: md2roff					
Affected Version(s): 1.7					
Out-of-bounds Write	02-Jul-2022	9.8	** DISPUTED ** md2roff 1.7 has a stack-based buffer overflow via a Markdown file containing a large number of consecutive characters to be processed. NOTE: the vendor's position is that the product is not intended for untrusted input. **CVE ID : CVE-2022-34913**	N/A	A-MD2-MD2R-200722/354
Vendor: mdweb_project					
Product: mdweb					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2015-05-07					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The mandoku/mdweb repository through 2015-05-07 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31542**	N/A	A-MDW-MDWE-200722/355
Vendor: Mediawiki					
Product: mediawiki					
Affected Version(s): * Up to (excluding) 1.35.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2022	6.1	An issue was discovered in MediaWiki before 1.35.7, 1.36.x and 1.37.x before 1.37.3, and 1.38.x before 1.38.1. XSS can occur in configurations that allow a JavaScript payload in a username. After account creation, when it sets the page title to "Welcome" followed by the username, the username is not escaped: SpecialCreateAccount::successfulAction() calls ::showSuccessPage() with a message as second parameter, and	https://phabricator.wikimedia.org/T308471	A-MED-MEDI-200722/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OutputPage::setPageTitle() uses text(). **CVE ID : CVE-2022-34911**		
Affected Version(s): * Up to (excluding) 1.37.3					
N/A	02-Jul-2022	6.1	An issue was discovered in MediaWiki before 1.37.3 and 1.38.x before 1.38.1. The contributions-title, used on Special:Contributions, is used as page title without escaping. Hence, in a non-default configuration where a username contains HTML entities, it won't be escaped. **CVE ID : CVE-2022-34912**	https://phabricator.wikimedia.org/T308473	A-MED-MEDI-200722/357
Affected Version(s): 1.38.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2022	6.1	An issue was discovered in MediaWiki before 1.35.7, 1.36.x and 1.37.x before 1.37.3, and 1.38.x before 1.38.1. XSS can occur in configurations that allow a JavaScript payload in a username. After account creation, when it sets the page title to "Welcome" followed by the username, the username is not escaped:	https://phabricator.wikimedia.org/T308471	A-MED-MEDI-200722/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SpecialCreateAccount ::successfulAction() calls ::showSuccessPage() with a message as second parameter, and OutputPage::setPageTitle() uses text(). **CVE ID : CVE-2022-34911**		
N/A	02-Jul-2022	6.1	An issue was discovered in MediaWiki before 1.37.3 and 1.38.x before 1.38.1. The contributions-title, used on Special:Contributions, is used as page title without escaping. Hence, in a non-default configuration where a username contains HTML entities, it won't be escaped. **CVE ID : CVE-2022-34912**	https://phabricator.wikimedia.org/T308473	A-MED-MEDI-200722/359
Affected Version(s): From (including) 1.36.0 Up to (excluding) 1.37.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2022	6.1	An issue was discovered in MediaWiki before 1.35.7, 1.36.x and 1.37.x before 1.37.3, and 1.38.x before 1.38.1. XSS can occur in configurations that allow a JavaScript payload in a username. After account creation,	https://phabricator.wikimedia.org/T308471	A-MED-MEDI-200722/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when it sets the page title to "Welcome" followed by the username, the username is not escaped: SpecialCreateAccount ::successfulAction() calls ::showSuccessPage() with a message as second parameter, and OutputPage::setPageTitle() uses text(). **CVE ID : CVE-2022-34911**		
Vendor: mercadoenlineaback_project					
Product: mercadoenlineaback					
Affected Version(s): * Up to (including) 2022-05-04					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The cheo0/MercadoEnLineaBack repository through 2022-05-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31505**	N/A	A-MER-MERC-200722/361
Vendor: mercury_sample_manager_project					
Product: mercury_sample_manager					
Affected Version(s): * Up to (including) 2021-04-20					
Improper Limitation of a Pathname to a Restricted	11-Jul-2022	9.3	The HolgerGraef/MSM repository through 2021-04-20 on GitHub allows absolute path	N/A	A-MER-MERC-200722/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31517**		
Vendor: Microsoft					
Product: edge_chromium					
Affected Version(s): * Up to (excluding) 103.0.1264.44					
Improper Privilege Management	07-Jul-2022	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30192, CVE-2022-33638, CVE-2022-33639. **CVE ID : CVE-2022-33680**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33680	A-MIC-EDGE-200722/363
Vendor: Microweber					
Product: microweber					
Affected Version(s): * Up to (excluding) 1.2.19					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jul-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.2.19. **CVE ID : CVE-2022-2280**	https://github.com/microweber/microweber/commit/9ebbb4dd35da74025ab6965f722829a7f8f86566, https://huntr.dev/bounties/22561bfd-a28f-474e-9bfd-7263c1b71133	A-MIC-MICR-200722/364
Improper Neutralization of Input During	04-Jul-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.2.19.	https://huntr.dev/bounties/882d6cf9-64f5-4614-a873-	A-MIC-MICR-200722/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2022-2300**	a3030473c817, https://github.com/microweber/microweber/commit/70b46e231e7b2c113666745a0ab6de9a8b7ef08e	
Affected Version(s): * Up to (excluding) 1.2.20					
N/A	11-Jul-2022	9.8	Business Logic Errors in GitHub repository microweber/microweber prior to 1.2.20. **CVE ID : CVE-2022-2368**	https://huntr.dev/bounties/a9595eda-a5e0-4717-8d64-b445ef83f452, https://github.com/microweber/microweber/commit/53c000ccd5602536e28b15d9630eb8261b04a302	A-MIC-MICR-200722/366
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2022	6.1	Prior to microweber/microweber v1.2.20, due to improper neutralization of input, an attacker can steal tokens to perform cross-site request forgery, fetch contents from same-site and redirect a user. **CVE ID : CVE-2022-2353**	https://github.com/microweber/microweber/commit/79c6914bab8c9da07ac950fda17648d08c68b130, https://huntr.dev/bounties/7782c095-9e8c-48b0-a7f5-3a8f52e8af52	A-MIC-MICR-200722/367
Vendor: mingsoft					
Product: mcms					
Affected Version(s): 5.2.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	01-Jul-2022	9.8	MCMS v5.2.8 was discovered to contain an arbitrary file upload vulnerability. **CVE ID : CVE-2022-31943**	N/A	A-MIN-MCMS-200722/368
Vendor: mini_tmall_project					
Product: mini_tmall					
Affected Version(s): 1.0					
Incorrect Permission Assignment for Critical Resource	06-Jul-2022	8.8	Mini-Tmall v1.0 is vulnerable to Insecure Permissions via tomcat-embed-jasper. **CVE ID : CVE-2022-30929**	N/A	A-MIN-MINI-200722/369
Vendor: modelconverter_project					
Product: modelconverter					
Affected Version(s): * Up to (including) 2021-04-26					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The ml-inory/ModelConverter repository through 2021-04-26 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31545**	N/A	A-MOD-MODE-200722/370
Vendor: momentjs					
Product: moment					
Affected Version(s): From (including) 2.18.0 Up to (excluding) 2.29.4					
N/A	06-Jul-2022	7.5	moment is a JavaScript date library for parsing, validating, manipulating, and	https://github.com/moment/moment/commit/9a3b5894f3d5d602948ac	A-MOM-MOME-200722/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			formatting dates. Affected versions of moment were found to use an inefficient parsing algorithm. Specifically using string-to-date parsing in moment (more specifically rfc2822 parsing, which is tried by default) has quadratic (N^2) complexity on specific inputs. Users may notice a noticeable slowdown is observed with inputs above 10k characters. Users who pass user-provided strings without sanity length checks to moment constructor are vulnerable to (Re)DoS attacks. The problem is patched in 2.29.4, the patch can be applied to all affected versions with minimal tweaking. Users are advised to upgrade. Users unable to upgrade should consider limiting date lengths accepted from user input. **CVE ID : CVE-2022-31129**	8a02e4ee528a49ca3a3, https://github.com/moment/moment/pull/6015#issuecomment-1152961973, https://github.com/moment/moment/security/advisories/GHSA-wc69-rhjr-hc9g	
Vendor: monorepo_project					
Product: monorepo					
Affected Version(s): * Up to (including) 2021-03-03					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The cinemaproject/monorepo repository through 2021-03-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31529**	N/A	A-MON-MONO-200722/372
Vendor: mosaic_project					
Product: mosaic					
Affected Version(s): 1.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The Niyaz-Mohamed/mosaic repository through 1.0.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31521**	N/A	A-MOS-MOSA-200722/373
Vendor: movie-review-sentiment-analysis_project					
Product: movie-review-sentiment-analysis					
Affected Version(s): * Up to (including) 2017-05-07					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The rohitnayak/movie-review-sentiment-analysis repository through 2017-05-07 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	N/A	A-MOV-MOVI-200722/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31554		
Vendor: mp-m08-interface_project					
Product: mp-m08-interface					
Affected Version(s): * Up to (including) 2020-12-10					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The joaopedro-fg/mp-m08-interface repository through 2020-12-10 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31538**	N/A	A-MP--MP-M-200722/375
Vendor: munhak					
Product: munhak-moa					
Affected Version(s): * Up to (excluding) 2022-05-03					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The woduq1414/munhak-moa repository before 2022-05-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31564**	https://github.com/woduq1414/munhak-moa/commit/e8f800373b20cb22de70c7a994325b8903877da0	A-MUN-MUNH-200722/376
Vendor: nesote					
Product: inout_homestay					
Affected Version(s): 2.2					
Improper Neutralization of Special	07-Jul-2022	7.5	Inout Homestay v2.2 was discovered to contain a SQL injection vulnerability	N/A	A-NES-INOU-200722/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			via the guests parameter at /index.php?page=search/rentals. **CVE ID : CVE-2022-32055**		
Vendor: newsletter_module_project					
Product: newsletter_module					
Affected Version(s): 3.0.2.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2022	9.8	Newsletter Module v3.x was discovered to contain a SQL injection vulnerability via the zemez_newsletter_email parameter at /index.php. **CVE ID : CVE-2022-31856**	N/A	A-NEW-NEWS-200722/378
Vendor: nextauth.js					
Product: next-auth					
Affected Version(s): * Up to (excluding) 3.29.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2022	6.1	NextAuth.js is a complete open source authentication solution for Next.js applications. An attacker can pass a compromised input to the e-mail [signin endpoint](https://next-auth.js.org/getting-started/rest-api#post-apiauthsigninprovider) that contains some malicious HTML, tricking the e-mail server to send it to the user, so they can perform a phishing	https://next-auth.js.org/getting-started/upgrade-v4, https://github.com/nextauthjs/next-auth/security/advisories/GHSA-pgjx-7f9g-9463, https://next-auth.js.org/providers/email#customizing-emails	A-NEX-NEXT-200722/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack. Eg.: `balazs@email.com, <a href="http://attacker.com">Before signing in, claim your money!</a>`. This was previously sent to `balazs@email.com`, and the content of the email containing a link to the attacker's site was rendered in the HTML. This has been remedied in the following releases, by simply not rendering that e-mail in the HTML, since it should be obvious to the receiver what e-mail they used: next-auth v3 users before version 3.29.8 are impacted. (We recommend upgrading to v4, as v3 is considered unmaintained. next-auth v4 users before version 4.9.0 are impacted. If for some reason you cannot upgrade, the workaround requires you to sanitize the `email` parameter that is passed to `sendVerificationRequest` and rendered in the HTML. If you haven't created a custom		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`sendVerificationRequest`, you only need to upgrade. Otherwise, make sure to either exclude `email` from the HTML body or efficiently sanitize it. **CVE ID : CVE-2022-31127**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.9.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2022	6.1	NextAuth.js is a complete open source authentication solution for Next.js applications. An attacker can pass a compromised input to the e-mail [signin endpoint](https://next-auth.js.org/getting-started/rest-api#post-apiauthsigninprovider) that contains some malicious HTML, tricking the e-mail server to send it to the user, so they can perform a phishing attack. Eg.: `balazs@email.com, <a href="http://attacker.com">Before signing in, claim your money!</a>`. This was previously sent to `balazs@email.com`, and the content of the email containing a link to the attacker's	https://next-auth.js.org/getting-started/upgrade-v4, https://github.com/nextauthjs/next-auth/security/advisories/GHSA-pgjx-7f9g-9463, https://next-auth.js.org/providers/email#customizing-emails	A-NEX-NEXT-200722/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			site was rendered in the HTML. This has been remedied in the following releases, by simply not rendering that e-mail in the HTML, since it should be obvious to the receiver what e-mail they used: next-auth v3 users before version 3.29.8 are impacted. (We recommend upgrading to v4, as v3 is considered unmaintained. next-auth v4 users before version 4.9.0 are impacted. If for some reason you cannot upgrade, the workaround requires you to sanitize the `email` parameter that is passed to `sendVerificationRequest` and rendered in the HTML. If you haven't created a custom `sendVerificationRequest`, you only need to upgrade. Otherwise, make sure to either exclude `email` from the HTML body or efficiently sanitize it. **CVE ID : CVE-2022-31127**		
Vendor: Nextcloud					
Product: nextcloud_mail					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.12.2					
Improper Authentication	06-Jul-2022	4.3	Nextcloud mail is a Mail app for the Nextcloud home server product. Versions of Nextcloud mail prior to 1.12.2 were found to be missing user account ownership checks when performing tasks related to mail attachments. Attachments may have been exposed to incorrect system users. It is recommended that the Nextcloud Mail app is upgraded to 1.12.2. There are no known workarounds for this issue. ### Workarounds No workaround available ### References * [Pull request](https://github.com/nextcloud/mail/pull/6600) * [HackerOne](https://hackerone.com/reports/1579820) ### For more information If you have any questions or comments about this advisory: * Create a post in [nextcloud/security-advisories](https://github.com/nextcloud/security-advisories/discussion	https://github.com/nextcloud/mail/pull/6600/commits/6dd2527be8d4f6788b449c8a8f5577628b990605, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-xhv7-5mhv-299j, https://github.com/nextcloud/mail/pull/6600	A-NEX-NEXT-200722/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			s) * Customers: Open a support ticket at support.nextcloud.com **CVE ID : CVE-2022-31131**		
Product: nextcloud_server					
Affected Version(s): * Up to (excluding) 19.0.13.7					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jul-2022	3.5	Nextcloud server is an open source personal cloud server. Affected versions were found to be vulnerable to SMTP command injection. The impact varies based on which commands are supported by the backend SMTP server. However, the main risk here is that the attacker can then hijack an already-authenticated SMTP session and run arbitrary SMTP commands as the email user, such as sending emails to other users, changing the FROM user, and so on. As before, this depends on the configuration of the server itself, but newlines should be sanitized to mitigate such arbitrary SMTP command injection. It is recommended that the Nextcloud Server is upgraded to 22.2.8 ,	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-264h-3v4w-6xh2, https://hackerone.com/reports/1516377, https://github.com/nextcloud/server/pull/32428	A-NEX-NEXT-200722/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			23.0.5 or 24.0.1. There are no known workarounds for this issue. **CVE ID : CVE-2022-31014**		
Affected Version(s): * Up to (excluding) 22.2.8					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jul-2022	3.5	Nextcloud server is an open source personal cloud server. Affected versions were found to be vulnerable to SMTP command injection. The impact varies based on which commands are supported by the backend SMTP server. However, the main risk here is that the attacker can then hijack an already-authenticated SMTP session and run arbitrary SMTP commands as the email user, such as sending emails to other users, changing the FROM user, and so on. As before, this depends on the configuration of the server itself, but newlines should be sanitized to mitigate such arbitrary SMTP command injection. It is recommended that the Nextcloud Server is upgraded to 22.2.8 , 23.0.5 or 24.0.1. There are no known	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-264h-3v4w-6xh2, https://hackerone.com/reports/1516377, https://github.com/nextcloud/server/pull/32428	A-NEX-NEXT-200722/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this issue. **CVE ID : CVE-2022-31014**		
Affected Version(s): 24.0.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jul-2022	3.5	Nextcloud server is an open source personal cloud server. Affected versions were found to be vulnerable to SMTP command injection. The impact varies based on which commands are supported by the backend SMTP server. However, the main risk here is that the attacker can then hijack an already-authenticated SMTP session and run arbitrary SMTP commands as the email user, such as sending emails to other users, changing the FROM user, and so on. As before, this depends on the configuration of the server itself, but newlines should be sanitized to mitigate such arbitrary SMTP command injection. It is recommended that the Nextcloud Server is upgraded to 22.2.8 , 23.0.5 or 24.0.1. There are no known workarounds for this issue.	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-264h-3v4w-6xh2, https://hackerone.com/reports/1516377, https://github.com/nextcloud/server/pull/32428	A-NEX-NEXT-200722/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31014		
Affected Version(s): From (including) 20.0.0 Up to (excluding) 20.0.14.6					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jul-2022	3.5	Nextcloud server is an open source personal cloud server. Affected versions were found to be vulnerable to SMTP command injection. The impact varies based on which commands are supported by the backend SMTP server. However, the main risk here is that the attacker can then hijack an already-authenticated SMTP session and run arbitrary SMTP commands as the email user, such as sending emails to other users, changing the FROM user, and so on. As before, this depends on the configuration of the server itself, but newlines should be sanitized to mitigate such arbitrary SMTP command injection. It is recommended that the Nextcloud Server is upgraded to 22.2.8 , 23.0.5 or 24.0.1. There are no known workarounds for this issue. **CVE ID : CVE-2022-31014**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-264h-3v4w-6xh2, https://hackerone.com/reports/1516377, https://github.com/nextcloud/server/pull/32428	A-NEX-NEXT-200722/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 21.0.0 Up to (excluding) 21.0.9.5					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jul-2022	3.5	Nextcloud server is an open source personal cloud server. Affected versions were found to be vulnerable to SMTP command injection. The impact varies based on which commands are supported by the backend SMTP server. However, the main risk here is that the attacker can then hijack an already-authenticated SMTP session and run arbitrary SMTP commands as the email user, such as sending emails to other users, changing the FROM user, and so on. As before, this depends on the configuration of the server itself, but newlines should be sanitized to mitigate such arbitrary SMTP command injection. It is recommended that the Nextcloud Server is upgraded to 22.2.8 , 23.0.5 or 24.0.1. There are no known workarounds for this issue. **CVE ID : CVE-2022-31014**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-264h-3v4w-6xh2, https://hackerone.com/reports/1516377, https://github.com/nextcloud/server/pull/32428	A-NEX-NEXT-200722/386
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jul-2022	3.5	Nextcloud server is an open source personal cloud server. Affected versions were found to be vulnerable to SMTP command injection. The impact varies based on which commands are supported by the backend SMTP server. However, the main risk here is that the attacker can then hijack an already-authenticated SMTP session and run arbitrary SMTP commands as the email user, such as sending emails to other users, changing the FROM user, and so on. As before, this depends on the configuration of the server itself, but newlines should be sanitized to mitigate such arbitrary SMTP command injection. It is recommended that the Nextcloud Server is upgraded to 22.2.8 , 23.0.5 or 24.0.1. There are no known workarounds for this issue. **CVE ID : CVE-2022-31014**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-264h-3v4w-6xh2, https://hackerone.com/reports/1516377, https://github.com/nextcloud/server/pull/32428	A-NEX-NEXT-200722/387
Vendor: ninjateam					
Product: wp_duplicate_page					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2022	4.8	The WP Duplicate Page WordPress plugin before 1.3 does not sanitize and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed. **CVE ID : CVE-2022-2093**	N/A	A-NIN-WP_D-200722/388
Vendor: northern.tech					
Product: mender					
Affected Version(s): 3.2.0					
Incorrect Authorization	06-Jul-2022	4.3	The client in Northern.tech Mender 3.2.0, 3.2.1, and 3.2.2 has Incorrect Access Control. It listens on a random, unprivileged TCP port and exposes an HTTP proxy to facilitate API calls from additional client components running on the device. However, it listens on all network interfaces instead of only the localhost interface. Therefore, any client on the same network can connect to this TCP port and send HTTP requests. The Mender Client will forward these	https://mender.io/blog/cve-2022-32290-mender-client-listening-on-all-the-interfaces, https://northern.tech	A-NOR-MEND-200722/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests to the Mender Server. Additionally, if mTLS is set up, the Mender Client will connect to the Mender Server using the device's client certificate, making it possible for the attacker to bypass mTLS authentication and send requests to the Mender Server without direct access to the client certificate and related private key. Accessing the HTTP proxy from the local network doesn't represent a direct threat, because it doesn't expose any device or server-specific data. However, it increases the attack surface and can be a potential vector to exploit other vulnerabilities both on the Client and the Server. **CVE ID : CVE-2022-32290**		
Affected Version(s): 3.2.1					
Incorrect Authorization	06-Jul-2022	4.3	The client in Northern.tech Mender 3.2.0, 3.2.1, and 3.2.2 has Incorrect Access Control. It listens on a random, unprivileged TCP port and exposes an HTTP proxy to	https://mender.io/blog/cve-2022-32290-mender-client-listening-on-all-the-interfaces, https://northern.tech	A-NOR-MEND-200722/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			facilitate API calls from additional client components running on the device. However, it listens on all network interfaces instead of only the localhost interface. Therefore, any client on the same network can connect to this TCP port and send HTTP requests. The Mender Client will forward these requests to the Mender Server. Additionally, if mTLS is set up, the Mender Client will connect to the Mender Server using the device's client certificate, making it possible for the attacker to bypass mTLS authentication and send requests to the Mender Server without direct access to the client certificate and related private key. Accessing the HTTP proxy from the local network doesn't represent a direct threat, because it doesn't expose any device or server-specific data. However, it increases the attack surface and can be a potential vector to exploit other vulnerabilities		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			both on the Client and the Server. **CVE ID : CVE-2022-32290**		
Affected Version(s): 3.2.2					
Incorrect Authorization	06-Jul-2022	4.3	The client in Northern.tech Mender 3.2.0, 3.2.1, and 3.2.2 has Incorrect Access Control. It listens on a random, unprivileged TCP port and exposes an HTTP proxy to facilitate API calls from additional client components running on the device. However, it listens on all network interfaces instead of only the localhost interface. Therefore, any client on the same network can connect to this TCP port and send HTTP requests. The Mender Client will forward these requests to the Mender Server. Additionally, if mTLS is set up, the Mender Client will connect to the Mender Server using the device's client certificate, making it possible for the attacker to bypass mTLS authentication and send requests to the Mender Server without direct access	https://mender.io/blog/cve-2022-32290-mender-client-listening-on-all-the-interfaces, https://northern.tech	A-NOR-MEND-200722/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the client certificate and related private key. Accessing the HTTP proxy from the local network doesn't represent a direct threat, because it doesn't expose any device or server-specific data. However, it increases the attack surface and can be a potential vector to exploit other vulnerabilities both on the Client and the Server. **CVE ID : CVE-2022-32290**		
Vendor: nurse_quest_project					
Product: nurse_quest					
Affected Version(s): * Up to (including) 2018-02-22					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The romain20100/nursequest repository through 2018-02-22 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31555**	N/A	A-NUR-NURS-200722/392
Vendor: Nvidia					
Product: nvflare					
Affected Version(s): * Up to (excluding) 2.1.2					
Deserialization of	01-Jul-2022	9.8	NVFLARE, versions prior to 2.1.2, contains a vulnerability in its	N/A	A-NVI-NVFL-200722/393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			PKI implementation module, where The CA credentials are transported via pickle and no safe deserialization. The deserialization of Untrusted Data may allow an unprivileged network attacker to cause Remote Code Execution, Denial Of Service, and Impact to both Confidentiality and Integrity. **CVE ID : CVE-2022-31604**		
Deserialization of Untrusted Data	01-Jul-2022	9.8	NVFLARE, versions prior to 2.1.2, contains a vulnerability in its utils module, where YAML files are loaded via yaml.load() instead of yaml.safe_load(). The deserialization of Untrusted Data, may allow an unprivileged network attacker to cause Remote Code Execution, Denial Of Service, and Impact to both Confidentiality and Integrity. **CVE ID : CVE-2022-31605**	N/A	A-NVI-NVFL-200722/394
Vendor: Omron					
Product: sysmac_studio					
Affected Version(s): * Up to (including) 1.49					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	A-OMR-SYSM-200722/395
Authentication Bypass by	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-	A-OMR-SYSM-200722/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	2022-001_en.pdf	
Vendor: online_accreditation_management_system_project					
Product: online_accreditation_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jul-2022	9.8	Online Accreditation Management v1.0 was discovered to contain a SQL injection vulnerability via the USERNAME parameter at process.php. **CVE ID : CVE-2022-32056**	N/A	A-ONL-ONLI-200722/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: onyxforum_project					
Product: onyxforum					
Affected Version(s): * Up to (including) 2022-05-04					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The ChaoticOnyx/OnyxForum repository before 2022-05-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31501**	https://github.com/ChaoticOnyx/OnyxForum/commit/f25543dfc62a9694d7e4f67eebfa45e3de916053	A-ONY-ONYX-200722/398
Vendor: openssh_key_parser_project					
Product: openssh_key_parser					
Affected Version(s): * Up to (excluding) 0.0.6					
Generation of Error Message Containing Sensitive Information	06-Jul-2022	6.5	openssh_key_parser is an open source Python package providing utilities to parse and pack OpenSSH private and public key files. In versions prior to 0.0.6 if a field of a key is shorter than it is declared to be, the parser raises an error with a message containing the raw field value. An attacker able to modify the declared length of a key's sensitive field can thus expose the raw value of that field. Users are advised to upgrade to version	https://github.com/scottcwang/openssh_key_parser/commit/d5b53b4b7e76c5b666fc657019dbf864fb04076c, https://github.com/scottcwang/openssh_key_parser/security/advisories/GHSA-hm37-9xh2-q499	A-OPE-OPEN-200722/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.0.6, which no longer includes the raw field value in the error message. There are no known workarounds for this issue. **CVE ID : CVE-2022-31124**		
Vendor: Openssl					
Product: openssl					
Affected Version(s): 3.0.4					
Out-of-bounds Write	01-Jul-2022	9.8	The OpenSSL 3.0.4 release introduced a serious bug in the RSA implementation for X86_64 CPUs supporting the AVX512IFMA instructions. This issue makes the RSA implementation with 2048 bit private keys incorrect on such machines and memory corruption will happen during the computation. As a consequence of the memory corruption an attacker may be able to trigger a remote code execution on the machine performing the computation. SSL/TLS servers or other servers using 2048 bit RSA private keys running on machines supporting AVX512IFMA	https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=4d8a88c134df634ba610ff8db1eb8478ac5fd345, https://github.com/openssl/openssl/issues/18625, https://www.openssl.org/news/secadv/20220705.txt	A-OPE-OPEN-200722/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			instructions of the X86_64 architecture are affected by this issue. **CVE ID : CVE-2022-2274**		
Affected Version(s): From (including) 1.1.1 Up to (excluding) 1.1.1q					
Inadequate Encryption Strength	05-Jul-2022	7.5	AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p). **CVE ID : CVE-2022-2097**	https://www.openssl.org/news/secadv/20220705.txt, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=a98f339ddd7e8f487d6e0088d4a9a42324885a93, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=919925673d6c9cfed3c1085497f5dfbbed5fc431	A-OPE-OPEN-200722/401
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.5					
Inadequate Encryption Strength	05-Jul-2022	7.5	AES OCB mode for 32-bit x86 platforms using the AES-NI	https://www.openssl.org/news/secadv/20	A-OPE-OPEN-200722/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p). **CVE ID : CVE-2022-2097**	220705.txt, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=a98f339ddd7e8f487d6e0088d4a9a42324885a93, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=919925673d6c9cfed3c1085497f5dfbbed5fc431	
Vendor: Openvpn					
Product: openvpn_access_server					
Affected Version(s): * Up to (excluding) 2.11.0					
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	06-Jul-2022	7.5	OpenVPN Access Server before 2.11 uses a weak random generator used to create user session token for the web portal **CVE ID : CVE-2022-33738**	https://openvpn.net/vpn-server-resources/release-notes/#openvpn-access-server-2-11-0	A-OPE-OPEN-200722/403
Affected Version(s): From (including) 2.10.0 Up to (excluding) 2.11.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	06-Jul-2022	7.5	The OpenVPN Access Server installer creates a log file readable for everyone, which from version 2.10.0 and before 2.11.0 may contain a random generated admin password **CVE ID : CVE-2022-33737**	https://openvpn.net/vpn-server-resources/release-notes/	A-OPE-OPEN-200722/404
Vendor: orchest					
Product: orchest					
Affected Version(s): * Up to (excluding) 2022.05.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The orchest/orchest repository before 2022.05.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31503**	https://github.com/orchest/orchest/pull/913	A-ORC-ORCH-200722/405
Vendor: otfcc_project					
Product: otfcc					
Affected Version(s): 0.10.4					
Out-of-bounds Write	06-Jul-2022	9.8	OTFCC v0.10.4 was discovered to contain a heap buffer overflow after free via otfccbuild.c. **CVE ID : CVE-2022-33047**	N/A	A-OTF-OTFC-200722/406
Vendor: paddlepaddle					
Product: anakin					
Affected Version(s): * Up to (including) 0.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The PaddlePaddle/Anakin repository through 0.1.1 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31523**	N/A	A-PAD-ANAK-200722/407
Vendor: pagebar_project					
Product: pagebar					
Affected Version(s): * Up to (including) 2.65					
Cross-Site Request Forgery (CSRF)	11-Jul-2022	5.4	The Pagebar WordPress plugin through 2.65 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack. Furthermore, due to the lack of sanitisation in some of them, it could also lead to Stored XSS issues **CVE ID : CVE-2022-1757**	N/A	A-PAG-PAGE-200722/408
Vendor: parity					
Product: frontier					
Affected Version(s): -					
Always-Incorrect Control Flow	06-Jul-2022	5.3	Frontier is Substrate's Ethereum compatibility layer. In affected versions the truncation done when converting between	https://github.com/paritytech/frontier/pull/753, https://github.com/paritytec	A-PAR-FRON-200722/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Implement ation			EVM balance type and Substrate balance type was incorrectly implemented. This leads to possible discrepancy between appeared EVM transfer value and actual Substrate value transferred. It is recommended that an emergency upgrade to be planned and EVM execution temporarily paused in the mean time. The issue is patched in Frontier master branch commit fed5e0a9577c10bea021721e8c2c5c378e16bf66 and polkadot-v0.9.22 branch commit e3e427fa2e5d1200a784679f8015d4774cedc934. This vulnerability affects only EVM internal states, but not Substrate balance states or node. You can temporarily pause EVM execution (by setting up a Substrate `CallFilter` that disables `pallet-evm` and `pallet-ethereum` calls before the patch can be applied. **CVE ID : CVE-2022-31111**	h/frontier/security/advisories/GHSA-hc8w-mx86-9fcj, https://github.com/paritytech/frontier/commit/e3e427fa2e5d1200a784679f8015d4774cedc934	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: passport_project					
Product: passport					
Affected Version(s): * Up to (excluding) 0.6.0					
Session Fixation	01-Jul-2022	4.8	This affects the package passport before 0.6.0. When a user logs in or logs out, the session is regenerated instead of being closed. **CVE ID : CVE-2022-25896**	https://github.com/jaredhanson/passport/pull/900, https://snyk.io/vuln/SNYK-JS-PASSPORT-2840631, https://github.com/jaredhanson/passport/commit/7e9b9cf4d7be02428e963fc729496a45baeea608	A-PAS-PASS-200722/410
Vendor: pdfalto_project					
Product: pdfalto					
Affected Version(s): 0.4					
Out-of-bounds Write	01-Jul-2022	9.8	PDFAlto v0.4 was discovered to contain a heap buffer overflow via the component /pdfalto/src/pdfalto.cc. **CVE ID : CVE-2022-32324**	N/A	A-PDF-PDFA-200722/411
Vendor: photo_tag_project					
Product: photo_tag					
Affected Version(s): * Up to (including) 2020-08-31					
Improper Limitation of a Pathname to a Restricted Directory	11-Jul-2022	9.3	The uncleYiba/photo_tag repository through 2020-08-31 on GitHub allows absolute path traversal because the	N/A	A-PHO-PHOT-200722/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			Flask send_file function is used unsafely. **CVE ID : CVE-2022-31560**		
Vendor: portswigger					
Product: burp_suite					
Affected Version(s): * Up to (excluding) 2022.6					
Exposure of Resource to Wrong Sphere	08-Jul-2022	4.3	A URL disclosure issue was discovered in Burp Suite before 2022.6. If a user views a crafted response in the Repeater or Intruder, it may be incorrectly interpreted as a redirect. **CVE ID : CVE-2022-35406**	https://portswigger.net/burp/releases/professional-community-2022-6?requestededition=professional	A-POR-BURP-200722/413
Vendor: priority-software					
Product: priority					
Affected Version(s): * Up to (excluding) 22.0					
Authorization Bypass Through User-Controlled Key	06-Jul-2022	6.3	this vulnerability affect user that even not allowed to access via the web interface. First of all, the attacker needs to access the "Login menu - demo site" then he can see in this menu all the functionality of the application. If the attacker will try to click on one of the links, he will get an answer that he is not authorized because he needs to log in	N/A	A-PRI-PRIO-200722/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with credentials. after he performed log in to the system there are some functionalities that the specific user is not allowed to perform because he was configured with low privileges however all the attacker need to do in order to achieve his goals is to change the value of the prog step parameter from 0 to 1 or more and then the attacker could access to some of the functionality the web application that he couldn't perform it before the parameter changed. **CVE ID : CVE-2022-23173**		
Weak Password Recovery Mechanism for Forgotten Password	06-Jul-2022	4.3	An attacker can access to "Forgot my password" button, as soon as he puts users is valid in the system, the system would issue a message that a password reset email had been sent to user. This way you can verify which users are in the system and which are not. **CVE ID : CVE-2022-23172**	N/A	A-PRI-PRIO-200722/415
Vendor: projects_project					
Product: projects					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2022-04-03					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The RipudamanKaushikDal/projects repository through 2022-04-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31569**	N/A	A-PRO-PROJ-200722/416
Vendor: purestorage					
Product: pure_swagger					
Affected Version(s): * Up to (including) 1.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The PureStorage-OpenConnect/swagger repository through 1.1.5 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31524**	N/A	A-PUR-PURE-200722/417
Vendor: python-flask-restful-api_project					
Product: python-flask-restful-api					
Affected Version(s): * Up to (including) 2019-09-16					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The akashtalole/python-flask-restful-api repository through 2019-09-16 on GitHub allows absolute path traversal because the Flask send_file	N/A	A-PYT-PYTH-200722/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function is used unsafely. **CVE ID : CVE-2022-31571**		
Vendor: python-recipe-database_project					
Product: python-recipe-database					
Affected Version(s): * Up to (including) 2021-03-31					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The JustAnotherSoftware Developer/Python-Recipe-Database repository through 2021-03-31 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31518**	N/A	A-PYT-PYTH-200722/419
Vendor: pythonweb_project					
Product: pythonweb					
Affected Version(s): * Up to (including) 2018-10-31					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The echoleegroup/Python Web repository through 2018-10-31 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31534**	N/A	A-PYT-PYTH-200722/420
Vendor: python_athena_stack_project					
Product: python_athena_stack					
Affected Version(s): * Up to (including) 2019-11-08					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The olmax99/pyathenastack repository through 2019-11-08 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31550**	N/A	A-PYT-PYTH-200722/421
Vendor: quic-go_project					
Product: quic-go					
Affected Version(s): * Up to (including) 0.27.0					
Uncontrolled Resource Consumption	06-Jul-2022	7.5	** DISPUTED ** quic-go through 0.27.0 allows remote attackers to cause a denial of service (CPU consumption) via a Slowloris variant in which incomplete QUIC or HTTP/3 requests are sent. This occurs because mtu_discoverer.go misparses the MTU Discovery service and consequently overflows the probe timer. NOTE: the vendor's position is that this behavior should not be listed as a vulnerability on the CVE List. **CVE ID : CVE-2022-30591**	N/A	A-QUI-QUIC-200722/422
Vendor: realestate_project					
Product: realestate					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2018-11-30					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The deepaliupadhyay/RealEstate repository through 2018-11-30 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31574**	N/A	A-REA-REAL-200722/423
Vendor: Redhat					
Product: keycloak					
Affected Version(s): * Up to (excluding) 18.0.0					
Missing Authorization	08-Jul-2022	9.8	A privilege escalation flaw was found in the token exchange feature of keycloak. Missing authorization allows a client application holding a valid access token to exchange tokens for any target client by passing the client_id of the target. This could allow a client to gain unauthorized access to additional services. **CVE ID : CVE-2022-1245**	N/A	A-RED-KEYC-200722/424
Vendor: redirection-for-contact-form7					
Product: redirection_for_contact_form_7					
Affected Version(s): * Up to (excluding) 2.5.0					
Improper Neutralization of	04-Jul-2022	6.1	The Redirection for Contact Form 7 WordPress plugin	N/A	A-RED-REDI-200722/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			before 2.5.0 does not escape a link generated before outputting it in an attribute, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-0250**		
Vendor: rename_wp-login_project					
Product: rename_wp-login					
Affected Version(s): * Up to (including) 2.6.0					
Cross-Site Request Forgery (CSRF)	11-Jul-2022	6.5	The Rename wp-login.php WordPress plugin through 2.6.0 does not have CSRF check in place when updating the secret login URL, which could allow attackers to make a logged in admin change them via a CSRF attack **CVE ID : CVE-2022-1732**	N/A	A-REN-RENA-200722/426
Vendor: rexians					
Product: rex-web					
Affected Version(s): * Up to (including) 2022-06-05					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The Rexians/rex-web repository through 2022-06-05 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31568**	N/A	A-REX-REX--200722/427
Vendor: roxy-wi					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: roxy-wi					
Affected Version(s): * Up to (excluding) 6.1.1.0					
Improper Authentication	06-Jul-2022	9.8	Roxy-wi is an open source web interface for managing Haproxy, Nginx, Apache and Keepalived servers. A vulnerability in Roxy-wi allows a remote, unauthenticated attacker to bypass authentication and access admin functionality by sending a specially crafted HTTP request. This affects Roxywi versions before 6.1.1.0. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-31125**	https://github.com/hap-wi/roxy-wi/security/advisories/GHSA-hr76-3hxp-5mm3	A-ROX-ROXY-200722/428
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Jul-2022	9.8	Roxy-wi is an open source web interface for managing Haproxy, Nginx, Apache and Keepalived servers. A vulnerability in Roxy-wi allows a remote, unauthenticated attacker to code execution by sending a specially crafted HTTP request to /app/options.py file. This affects Roxy-wi versions before 6.1.1.0. Users are	https://github.com/hap-wi/roxy-wi/security/advisories/GHSA-mh86-878h-43c9	A-ROX-ROXY-200722/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-31126**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jul-2022	9.8	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. Versions prior to 6.1.1.0 are subject to a remote code execution vulnerability. System commands can be run remotely via the subprocess_execute function without processing the inputs received from the user in the /app/options.py file. Attackers need not be authenticated to exploit this vulnerability. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2022-31137**	https://github.com/hap-wi/roxy-wi/security/advisories/GHSA-53r2-mq99-f532, https://github.com/hap-wi/roxy-wi/commit/82666df1e60c45dd6aa533b01a392f015d32f755	A-ROX-ROXY-200722/430
Vendor: rpc.py_project					
Product: rpc.py					
Affected Version(s): From (including) 0.4.2 Up to (including) 0.6.0					
N/A	08-Jul-2022	9.8	rpc.py through 0.6.0 allows Remote Code Execution because an unpickle occurs when the "serializer: pickle"	https://github.com/abersheeran/rpc.py/commit/491e7a841ed9a754796d	A-RPC-RPC.-200722/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP header is sent. In other words, although JSON (not Pickle) is the default data format, an unauthenticated client can cause the data to be processed with unpickle. **CVE ID : CVE-2022-35411**	6ab047a9fb16e23bf8bd	
Vendor: s3label_project					
Product: s3label					
Affected Version(s): * Up to (including) 2019-08-14					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The stonethree/s3label repository through 2019-08-14 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31584**	N/A	A-S3L-S3LA-200722/432
Vendor: Samsung					
Product: find_my_mobile					
Affected Version(s): * Up to (excluding) 7.2.24.12					
Use of Insufficiently Random Values	12-Jul-2022	5.3	Improper identifier creation logic in Find My Mobile prior to version 7.2.24.12 allows attacker to identify the device. **CVE ID : CVE-2022-33707**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=07	A-SAM-FIND-200722/433
Product: galaxy_store					
Affected Version(s): * Up to (excluding) 4.5.41.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jul-2022	7.8	Improper input validation vulnerability in AppsPackageInstaller in Galaxy Store prior to version 4.5.41.8 allows local attackers to launch activities as Galaxy Store privilege. **CVE ID : CVE-2022-33708**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=07	A-SAM-GALA-200722/434
Improper Privilege Management	12-Jul-2022	7.8	Improper input validation vulnerability in ApexPackageInstaller in Galaxy Store prior to version 4.5.41.8 allows local attackers to launch activities as Galaxy Store privilege. **CVE ID : CVE-2022-33709**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=07	A-SAM-GALA-200722/435
Improper Privilege Management	12-Jul-2022	7.8	Improper input validation vulnerability in BillingPackageInsraller in Galaxy Store prior to version 4.5.41.8 allows local attackers to launch activities as Galaxy Store privilege. **CVE ID : CVE-2022-33710**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=07	A-SAM-GALA-200722/436
Product: samsung_gallery					
Affected Version(s): * Up to (excluding) 13.1.05.8					
N/A	12-Jul-2022	2.4	Improper access control vulnerability in Samsung Gallery	https://security.samsungmobile.com/service	A-SAM-SAMS-200722/437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to version 13.1.05.8 allows physical attackers to access the pictures using S Pen air gesture. **CVE ID : CVE-2022-33706**	Web.smsb?year==2022&month=07	
Vendor: SAP					
Product: businessobjects_business_intelligence_platform					
Affected Version(s): 420					
N/A	12-Jul-2022	8.8	SAP BusinessObjects CMC allows an unauthenticated attacker to retrieve token information over the network which would otherwise be restricted. This can be achieved only when a legitimate user accesses the application and a local compromise occurs, like sniffing or social engineering. On successful exploitation, the attacker can completely compromise the application. **CVE ID : CVE-2022-35228**	https://launchpad.support.sap.com/#/notes/3221288, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-200722/438
Incorrect Authorization	12-Jul-2022	6.5	Under certain conditions SAP BusinessObjects Business Intelligence Platform 4.x - versions 420,430 allows user	https://launchpad.support.sap.com/#/notes/3169239, https://www.sap.com/documents/2022/02/	A-SAP-BUSI-200722/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator to view, edit or modify rights of objects it doesn't own and which would otherwise be restricted. **CVE ID : CVE-2022-29619**	fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 430					
N/A	12-Jul-2022	8.8	SAP BusinessObjects CMC allows an unauthenticated attacker to retrieve token information over the network which would otherwise be restricted. This can be achieved only when a legitimate user accesses the application and a local compromise occurs, like sniffing or social engineering. On successful exploitation, the attacker can completely compromise the application. **CVE ID : CVE-2022-35228**	https://launchpad.support.sap.com/#/notes/3221288, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-200722/440
Incorrect Authorization	12-Jul-2022	6.5	Under certain conditions SAP BusinessObjects Business Intelligence Platform 4.x - versions 420,430 allows user Administrator to	https://launchpad.support.sap.com/#/notes/3169239, https://www.sap.com/documents/2022/02/fa865ea4-	A-SAP-BUSI-200722/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			view, edit or modify rights of objects it doesn't own and which would otherwise be restricted. **CVE ID : CVE-2022-29619**	167e-0010-bca6-c68f7e60039b.html	
Product: businessobjects_bw_publisher_service					
Affected Version(s): 420					
Unquoted Search Path or Element	12-Jul-2022	7.8	SAP BusinessObjects BW Publisher Service - versions 420, 430, uses a search path that contains an unquoted element. A local attacker can gain elevated privileges by inserting an executable file in the path of the affected service **CVE ID : CVE-2022-31591**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3167430	A-SAP-BUSI-200722/442
Affected Version(s): 430					
Unquoted Search Path or Element	12-Jul-2022	7.8	SAP BusinessObjects BW Publisher Service - versions 420, 430, uses a search path that contains an unquoted element. A local attacker can gain elevated privileges by inserting an executable file in the path of the affected service **CVE ID : CVE-2022-31591**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3167430	A-SAP-BUSI-200722/443
Product: business_objects_business_intelligence_platform					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 420					
Insufficient Verification of Data Authenticity	12-Jul-2022	5.4	Due to insufficient input validation, SAP Business Objects - version 420, allows an authenticated attacker to submit a malicious request through an allowed operation. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2022-31598**	https://launchpad.support.sap.com/#/notes/3213279, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-200722/444
Product: business_one					
Affected Version(s): 10.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Jul-2022	8.8	SAP Business One client - version 10.0 allows an attacker with low privileges, to inject code that can be executed by the application. An attacker could thereby control the behavior of the application. **CVE ID : CVE-2022-31593**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3191012	A-SAP-BUSI-200722/445
Product: enterprise_extension_defense_forces_\&_public_security					
Affected Version(s): 605					
Missing Authorization	12-Jul-2022	4.3	The application SAP Enterprise Extension Defense Forces &	https://launchpad.support.sap.com/#/notes	A-SAP-ENTE-200722/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Public Security - versions 605, 606, 616,617,618, 802, 803, 804, 805, 806, does not perform necessary authorization checks for an authenticated user over the network, resulting in escalation of privileges leading to a limited impact on confidentiality. **CVE ID : CVE-2022-31592**	/3196280, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 606					
Missing Authorization	12-Jul-2022	4.3	The application SAP Enterprise Extension Defense Forces & Public Security - versions 605, 606, 616,617,618, 802, 803, 804, 805, 806, does not perform necessary authorization checks for an authenticated user over the network, resulting in escalation of privileges leading to a limited impact on confidentiality. **CVE ID : CVE-2022-31592**	https://launchpad.support.sap.com/#/notes/3196280, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ENTE-200722/447
Affected Version(s): 616					
Missing Authorization	12-Jul-2022	4.3	The application SAP Enterprise Extension Defense Forces & Public Security - versions 605, 606,	https://launchpad.support.sap.com/#/notes/3196280, https://www.s	A-SAP-ENTE-200722/448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			616,617,618, 802, 803, 804, 805, 806, does not perform necessary authorization checks for an authenticated user over the network, resulting in escalation of privileges leading to a limited impact on confidentiality. **CVE ID : CVE-2022-31592**	ap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 617					
Missing Authorization	12-Jul-2022	4.3	The application SAP Enterprise Extension Defense Forces & Public Security - versions 605, 606, 616,617,618, 802, 803, 804, 805, 806, does not perform necessary authorization checks for an authenticated user over the network, resulting in escalation of privileges leading to a limited impact on confidentiality. **CVE ID : CVE-2022-31592**	https://launchpad.support.sap.com/#/notes/3196280, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ENTE-200722/449
Affected Version(s): 618					
Missing Authorization	12-Jul-2022	4.3	The application SAP Enterprise Extension Defense Forces & Public Security - versions 605, 606, 616,617,618, 802, 803, 804, 805, 806,	https://launchpad.support.sap.com/#/notes/3196280, https://www.sap.com/documents/2022/02/	A-SAP-ENTE-200722/450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not perform necessary authorization checks for an authenticated user over the network, resulting in escalation of privileges leading to a limited impact on confidentiality. **CVE ID : CVE-2022-31592**	fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 802					
Missing Authorization	12-Jul-2022	4.3	The application SAP Enterprise Extension Defense Forces & Public Security - versions 605, 606, 616,617,618, 802, 803, 804, 805, 806, does not perform necessary authorization checks for an authenticated user over the network, resulting in escalation of privileges leading to a limited impact on confidentiality. **CVE ID : CVE-2022-31592**	https://launchpad.support.sap.com/#/notes/3196280, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ENTE-200722/451
Affected Version(s): 803					
Missing Authorization	12-Jul-2022	4.3	The application SAP Enterprise Extension Defense Forces & Public Security - versions 605, 606, 616,617,618, 802, 803, 804, 805, 806, does not perform necessary	https://launchpad.support.sap.com/#/notes/3196280, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-	A-SAP-ENTE-200722/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authorization checks for an authenticated user over the network, resulting in escalation of privileges leading to a limited impact on confidentiality. **CVE ID : CVE-2022-31592**	bca6-c68f7e60039b.html	
Affected Version(s): 804					
Missing Authorization	12-Jul-2022	4.3	The application SAP Enterprise Extension Defense Forces & Public Security - versions 605, 606, 616,617,618, 802, 803, 804, 805, 806, does not perform necessary authorization checks for an authenticated user over the network, resulting in escalation of privileges leading to a limited impact on confidentiality. **CVE ID : CVE-2022-31592**	https://launchpad.support.sap.com/#/notes/3196280, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ENTE-200722/453
Affected Version(s): 805					
Missing Authorization	12-Jul-2022	4.3	The application SAP Enterprise Extension Defense Forces & Public Security - versions 605, 606, 616,617,618, 802, 803, 804, 805, 806, does not perform necessary authorization checks for an authenticated	https://launchpad.support.sap.com/#/notes/3196280, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-ENTE-200722/454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user over the network, resulting in escalation of privileges leading to a limited impact on confidentiality. **CVE ID : CVE-2022-31592**	c68f7e60039b.html	
Affected Version(s): 806					
Missing Authorization	12-Jul-2022	4.3	The application SAP Enterprise Extension Defense Forces & Public Security - versions 605, 606, 616,617,618, 802, 803, 804, 805, 806, does not perform necessary authorization checks for an authenticated user over the network, resulting in escalation of privileges leading to a limited impact on confidentiality. **CVE ID : CVE-2022-31592**	https://launchpad.support.sap.com/#/notes/3196280, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ENTE-200722/455
Vendor: scorelab					
Product: openmf					
Affected Version(s): * Up to (excluding) 2022-05-03					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The scorelab/OpenMF repository before 2022-05-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	N/A	A-SCO-OPEN-200722/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31581		
Vendor: scss-tokenizer_project					
Product: scss-tokenizer					
Affected Version(s): *					
N/A	01-Jul-2022	7.5	All versions of package scss-tokenizer are vulnerable to Regular Expression Denial of Service (ReDoS) via the loadAnnotation() function, due to the usage of insecure regex. **CVE ID : CVE-2022-25758**	https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2936782, https://snyk.io/vuln/SNYK-JS-SCSSTOKENIZER-2339884, https://github.com/sasstools/scss-tokenizer/issues/45	A-SCS-SCSS-200722/457
Vendor: setupbox_project					
Product: setupbox					
Affected Version(s): * Up to (including) 1.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The maxtortime/SetupBox repository through 1.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31543**	N/A	A-SET-SETU-200722/458
Vendor: shackerpanel_project					
Product: shackerpanel					
Affected Version(s): * Up to (including) 2021-05-25					
Improper Limitation	11-Jul-2022	9.3	The heidi-luong1109/shackerpa	N/A	A-SHA-SHAC-200722/459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			nel repository through 2021-05-25 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31576**		
Vendor: sharebar_project					
Product: sharebar					
Affected Version(s): * Up to (including) 1.4.1					
Cross-Site Request Forgery (CSRF)	11-Jul-2022	5.4	The Sharebar WordPress plugin through 1.4.1 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and also lead to Stored Cross-Site Scripting issue due to the lack of sanitisation and escaping in some of them **CVE ID : CVE-2022-1626**	N/A	A-SHA-SHAR-200722/460
Vendor: shiva-server_project					
Product: shiva-server					
Affected Version(s): * Up to (including) 0.10.0					
Improper Limitation of a Pathname to a Restricted	11-Jul-2022	9.3	The tooxie/shiva-server repository through 0.10.0 on GitHub allows absolute path traversal because the	N/A	A-SHI-SHIV-200722/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			Flask send_file function is used unsafely. **CVE ID : CVE-2022-31558**		
Vendor: shortcut_macros_project					
Product: shortcut_macros					
Affected Version(s): * Up to (including) 1.3					
Cross-Site Request Forgery (CSRF)	11-Jul-2022	6.5	The Shortcut Macros WordPress plugin through 1.3 does not have authorisation and CSRF checks in place when updating its settings, which could allow any authenticated users, such as subscriber, to update them. **CVE ID : CVE-2022-1956**	N/A	A-SHO-SHOR-200722/462
Vendor: Siemens					
Product: pads_viewer					
Affected Version(s): *					
Out-of-bounds Read	12-Jul-2022	7.8	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to execute code in the context of the current	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process. (FG-VD-22-037, FG-VD-22-059) **CVE ID : CVE-2022-34272**		
Out-of-bounds Write	12-Jul-2022	7.8	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-038) **CVE ID : CVE-2022-34273**	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/464
Out-of-bounds Write	12-Jul-2022	7.8	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-039) **CVE ID : CVE-2022-34274**	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Jul-2022	7.8	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-040) **CVE ID : CVE-2022-34275**	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/466
Out-of-bounds Write	12-Jul-2022	7.8	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-041) **CVE ID : CVE-2022-34276**	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/467
Out-of-bounds Read	12-Jul-2022	7.8	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of bounds read past the end of an allocated buffer when parsing PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-042) **CVE ID : CVE-2022-34277**		
Out-of-bounds Read	12-Jul-2022	7.8	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-043) **CVE ID : CVE-2022-34278**	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/469
Out-of-bounds Read	12-Jul-2022	7.8	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute code in the context of the current process. (FG-VD-22-044) **CVE ID : CVE-2022-34279**		
Out-of-bounds Read	12-Jul-2022	7.8	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to execute code in the context of the current process. (FG-VD-22-045) **CVE ID : CVE-2022-34280**	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/471
Out-of-bounds Read	12-Jul-2022	7.8	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to execute code in the context of the current	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process. (FG-VD-22-046) **CVE ID : CVE-2022-34281**		
Out-of-bounds Write	12-Jul-2022	7.8	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-049) **CVE ID : CVE-2022-34284**	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/473
Out-of-bounds Write	12-Jul-2022	7.8	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-051) **CVE ID : CVE-2022-34286**	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Jul-2022	7.8	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-054) **CVE ID : CVE-2022-34289**	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/475
Out-of-bounds Read	12-Jul-2022	5.5	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-047) **CVE ID : CVE-2022-34282**	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/476
Out-of-bounds Read	12-Jul-2022	5.5	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected	https://cert-portal.siemens.com/productce	A-SIE-PADS-200722/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-048) **CVE ID : CVE-2022-34283**	rt/pdf/ssa-439148.pdf	
Out-of-bounds Read	12-Jul-2022	5.5	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-050) **CVE ID : CVE-2022-34285**	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/478
Improper Restriction of Operations within the Bounds of	12-Jul-2022	5.5	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains a stack corruption vulnerability while	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-052, FG-VD-22-056) **CVE ID : CVE-2022-34287**		
Out-of-bounds Read	12-Jul-2022	5.5	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-053) **CVE ID : CVE-2022-34288**	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/480
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-Jul-2022	5.5	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains a stack corruption vulnerability while parsing PCB files. An attacker could leverage this vulnerability to leak information in the	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. (FG-VD-22-055) **CVE ID : CVE-2022-34290**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-Jul-2022	5.5	A vulnerability has been identified in PADS Standard/Plus Viewer (All versions). The affected application contains a stack corruption vulnerability while parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-057, FG-VD-22-058, FG-VD-22-060) **CVE ID : CVE-2022-34291**	https://cert-portal.siemens.com/productcert/pdf/ssa-439148.pdf	A-SIE-PADS-200722/482
Product: simcenter_femap					
Affected Version(s): * Up to (excluding) 2022.2					
Out-of-bounds Write	12-Jul-2022	7.8	A vulnerability has been identified in Simcenter Femap (All versions < V2022.2). The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17293)	https://cert-portal.siemens.com/productcert/pdf/ssa-474231.pdf	A-SIE-SIMC-200722/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34748		
Vendor: simple-rat_project					
Product: simple-rat					
Affected Version(s): * Up to (including) 2022-05-03					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The sergeKashkin/Simple-RAT repository before 2022-05-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31510**	https://github.com/sergeKashkin/Simple-RAT/pull/11	A-SIM-SIMP-200722/484
Vendor: simple_parking_management_system_project					
Product: simple_parking_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-2022	5.4	A vulnerability, which was classified as problematic, was found in SourceCodester Simple Parking Management System 1.0. This affects an unknown part of the file /ci_spms/admin/category. The manipulation of the argument vehicle_type with the input "><script>alert("XSS")</script> leads to cross site scripting. It is possible to initiate the attack remotely.	N/A	A-SIM-SIMP-200722/485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2022-2364**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-2022	4.6	A vulnerability, which was classified as problematic, has been found in SourceCodester Simple Parking Management System 1.0. Affected by this issue is some unknown functionality of the file /ci_spms/admin/search/searching/. The manipulation of the argument search with the input "><script>alert("XSS")</script> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2022-2363**	N/A	A-SIM-SIMP-200722/486
Vendor: simple_sales_management_system_project					
Product: simple_sales_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During	12-Jul-2022	5.4	A vulnerability classified as problematic was found in SourceCodester	N/A	A-SIM-SIMP-200722/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Simple Sales Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /ci_ssms/index.php/orders/create. The manipulation of the argument customer_name with the input <script>alert("XSS")</script> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2022-2293**		
Vendor: sleep_learner_project					
Product: sleep_learner					
Affected Version(s): * Up to (including) 2021-02-21					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The rainsoupah/sleep-learner repository through 2021-02-21 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31553**	N/A	A-SLE-SLEE-200722/488
Vendor: snipeitapp					
Product: snipe-it					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 6.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2022	4.8	An arbitrary file upload vulnerability in the Update Branding Settings component of Snipe-IT v6.0.2 allows attackers to execute arbitrary code via a crafted file. **CVE ID : CVE-2022-32060**	N/A	A-SNI-SNIP-200722/489
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2022	4.8	An arbitrary file upload vulnerability in the Select User function under the People Menu component of Snipe-IT v6.0.2 allows attackers to execute arbitrary code via a crafted file. **CVE ID : CVE-2022-32061**	N/A	A-SNI-SNIP-200722/490
Vendor: soflyy					
Product: wp_all_import					
Affected Version(s): * Up to (excluding) 3.6.8					
Improper Neutralization of Formula Elements in a CSV File	04-Jul-2022	7.2	The Import any XML or CSV File to WordPress plugin before 3.6.8 accepts all zip files and automatically extracts the zip file without validating the extracted file type. Allowing high privilege users such as admin to upload an arbitrary file like PHP, leading to RCE	N/A	A-SOF-WP_A-200722/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2268		
Vendor: solar-system-simulator_project					
Product: solar-system-simulator					
Affected Version(s): * Up to (including) 2021-07-26					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The jmcginty15/Solar-system-simulator repository through 2021-07-26 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31537**	N/A	A-SOL-SOLA-200722/492
Vendor: so_filter_shop_by_project					
Product: so_filter_shop_by					
Affected Version(s): 3.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2022	9.8	So Filter Shop v3.x was discovered to contain multiple blind SQL injection vulnerabilities via the att_value_id , manu_value_id , opt_value_id , and subcate_value_id parameters at /index.php?route=extension/module/so_filter_shop_by/filter_data. **CVE ID : CVE-2022-34972**	N/A	A-SO_-SO_F-200722/493
Vendor: sphere_imagebackend_project					
Product: sphere_imagebackend					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2019-10-03					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The varijkapil13/Sphere_ImageBackend repository through 2019-10-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31561**	N/A	A-SPH-SPHE-200722/494
Vendor: sphere_project					
Product: sphere					
Affected Version(s): * Up to (including) 2020-05-31					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The noamezekiel/sphere repository through 2020-05-31 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31547**	N/A	A-SPH-SPHE-200722/495
Vendor: sygnoos					
Product: popup_builder					
Affected Version(s): * Up to (excluding) 4.1.11					
Improper Neutralization of Input During Web Page Generation	11-Jul-2022	4.8	The Popup Builder WordPress plugin before 4.1.11 does not escape and sanitize some settings, which could allow high privilege users to perform Stored Cross-	N/A	A-SYG-POPU-200722/496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Site Scripting attacks when the unfiltred_html is disallowed **CVE ID : CVE-2022-1894**		
Vendor: Synology					
Product: calendar					
Affected Version(s): * Up to (excluding) 2.4.5-10930					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-2022	5.4	Improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability in Event Management in Synology Calendar before 2.4.5-10930 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **CVE ID : CVE-2022-22682**	https://www.synology.com/security/advisory/Synology_SA_22_07	A-SYN-CALE-200722/497
Product: photo_station					
Affected Version(s): * Up to (excluding) 6.8.16-3506					
Session Fixation	06-Jul-2022	7.5	Session fixation vulnerability in access control management in Synology Photo Station before 6.8.16-3506 allows remote attackers to bypass security constraint via unspecified vectors.	https://www.synology.com/security/advisory/Synology_SA_21_26	A-SYN-PHOT-200722/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22681		
Vendor: syntactics					
Product: free_booking_plugin_for_hotels\,_restaurant_and_car_rental					
Affected Version(s): * Up to (excluding) 1.1.16					
Unrestricted Upload of File with Dangerous Type	11-Jul-2022	9.8	The Free Booking Plugin for Hotels, Restaurant and Car Rental WordPress plugin before 1.1.16 suffers from insufficient input validation which leads to arbitrary file upload and subsequently to remote code execution. An AJAX action accessible to unauthenticated users is affected by this issue. An allowlist of valid file extensions is defined but is not used during the validation steps. **CVE ID : CVE-2022-1952**	N/A	A-SYN-FREE-200722/499
Vendor: syrabond_project					
Product: syrabond					
Affected Version(s): * Up to (including) 2020-05-25					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The yogson/syrabond repository through 2020-05-25 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.	N/A	A-SYR-SYRA-200722/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31565		
Vendor: testplatform_project					
Product: testplatform					
Affected Version(s): * Up to (including) 2016-07-19					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The zippies/testplatform repository through 2016-07-19 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31588**	N/A	A-TES-TEST-200722/501
Vendor: themeisle					
Product: wp_maintenance_mode_\&_coming_soon					
Affected Version(s): * Up to (excluding) 2.4.5					
Cross-Site Request Forgery (CSRF)	11-Jul-2022	6.5	The WP Maintenance Mode & Coming Soon WordPress plugin before 2.4.5 is lacking CSRF when emptying the subscribed users list, which could allow attackers to make a logged in admin perform such action via a CSRF attack **CVE ID : CVE-2022-1576**	N/A	A-THE-WP_M-200722/502
Vendor: thinkst					
Product: canarytokens					
Affected Version(s): * Up to (excluding) 2022-07-01					
Improper Neutralization of	01-Jul-2022	6.1	Canarytokens is an open source tool which helps track	https://github.com/thinkst/canarytokens/s	A-THI-CANA-200722/503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			activity and actions on your network. A Cross-Site Scripting vulnerability was identified in the history page of triggered Canarytokens. This permits an attacker who recognised an HTTP-based Canarytoken (a URL) to execute Javascript in the Canarytoken's history page (domain: canarytokens.org) when the history page is later visited by the Canarytoken's creator. This vulnerability could be used to disable or delete the affected Canarytoken, or view its activation history. It might also be used as a stepping stone towards revealing more information about the Canarytoken's creator to the attacker. For example, an attacker could recover the email address tied to the Canarytoken, or place Javascript on the history page that redirect the creator towards an attacker-controlled Canarytoken to show the creator's network location. An attacker	ecurity/advisories/GHSA-5675-3424-hpqr, https://github.com/thinkst/canarytokens/commit/dc378957bc28a6f3b5a8d7217b0605d81111f090	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could only act on the discovered Canarytoken. This issue did not expose other Canarytokens or other Canarytoken creators. The issue has been patched on Canarytokens.org and in the latest release. No signs of successful exploitation of this vulnerability have been found. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-31113**		
Vendor: thunderatz					
Product: thunderdocs					
Affected Version(s): * Up to (including) 2020-05-01					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The ThundeRatz/ThunderDocs repository through 2020-05-01 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31526**	N/A	A-THU-THUN-200722/504
Vendor: trainenergyserver_project					
Product: trainenergyserver					
Affected Version(s): * Up to (including) 2017-08-03					
Improper Limitation of a	11-Jul-2022	9.3	The rusyasoft/TrainEnergyServer repository	N/A	A-TRA-TRAI-200722/505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			through 2017-08-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31556**		
Vendor: travel_blahg_project					
Product: travel_blahg					
Affected Version(s): * Up to (including) 2016-01-16					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The dankolbman/travel_blahg repository through 2016-01-16 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31532**	N/A	A-TRA-TRAV-200722/506
Vendor: trilium_project					
Product: trilium					
Affected Version(s): * Up to (excluding) 0.52.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jul-2022	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository zadam/trilium prior to 0.52.4, 0.53.1-beta. **CVE ID : CVE-2022-2290**	https://github.com/zadam/trilium/commit/3faae63b849a1fabc31b823bb7af3a84d32256a7, https://huntr.dev/bounties/367c5c8d-ad6f-46be-8503-06648ecf09cf	A-TRI-TRIL-200722/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 0.53.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository zadam/trilium prior to 0.53.3. **CVE ID : CVE-2022-2365**	https://github.com/zadam/trilium/commit/1dfc37704fdd90ab7afbd8a586bdfc5cfaadeb8a, https://huntr.dev/bounties/34b281cd-ff4a-4ab0-ae25-56aef557682f	A-TRI-TRIL-200722/508
Vendor: typeorm					
Product: typeorm					
Affected Version(s): * Up to (excluding) 0.3.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jul-2022	9.8	** DISPUTED ** The findOne function in TypeORM before 0.3.0 can either be supplied with a string or a FindOneOptions object. When input to the function is a user-controlled parsed JSON object, supplying a crafted FindOneOptions instead of an id string leads to SQL injection. NOTE: the vendor's position is that the user's application is responsible for input validation. **CVE ID : CVE-2022-33171**	N/A	A-TYP-TYPE-200722/509
Vendor: ublock_origin_project					
Product: ublock_origin					
Affected Version(s): * Up to (excluding) 1.41.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jul-2022	6.1	Cross Site Scripting (XSS) vulnerability in uBlock Origin extension before 1.41.1 allows remote attackers to run arbitrary code via a spoofed 'MessageSender.url' to the browser renderer process. **CVE ID : CVE-2022-32308**	https://github.com/uBlockOrigin/uBlock-issues/issues/1992	A-UBL-UBLO-200722/510
Vendor: ultrajson_project					
Product: ultrajson					
Affected Version(s): * Up to (excluding) 5.4.0					
Always-Incorrect Control Flow Implementation	05-Jul-2022	7.5	UltraJSON is a fast JSON encoder and decoder written in pure C with bindings for Python 3.7+. Affected versions were found to improperly decode certain characters. JSON strings that contain escaped surrogate characters not part of a proper surrogate pair were decoded incorrectly. Besides corrupting strings, this allowed for potential key confusion and value overwriting in dictionaries. All users parsing JSON from untrusted sources are vulnerable. From version 5.4.0, UltraJSON decodes	https://github.com/ultrajson/ultrajson/commit/67ec07183342589d602e0fcf7bb1ff3e19272687, https://github.com/ultrajson/ultrajson/security/advisories/GHSA-wpqr-jcpx-745r	A-ULT-ULTR-200722/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lone surrogates in the same way as the standard library's `json` module does, preserving them in the parsed output. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-31116**		
Double Free	05-Jul-2022	5.9	UltraJSON is a fast JSON encoder and decoder written in pure C with bindings for Python 3.7+. In versions prior to 5.4.0 an error occurring while reallocating a buffer for string decoding can cause the buffer to get freed twice. Due to how UltraJSON uses the internal decoder, this double free is impossible to trigger from Python. This issue has been resolved in version 5.4.0 and all users should upgrade to UltraJSON 5.4.0. There are no known workarounds for this issue. **CVE ID : CVE-2022-31117**	https://github.com/ultrajson/ultrajson/security/advisories/GHSA-fm67-cv37-96ff, https://github.com/ultrajson/ultrajson/commit/9c20de0f77b391093967e25d01fb48671104b15b	A-ULT-ULTR-200722/512
Vendor: umbral_project					
Product: umbral					
Affected Version(s): * Up to (including) 2020-01-15					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The decentraminds/umbral repository through 2020-01-15 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31533**	N/A	A-UMB-UMBR-200722/513
Vendor: varktech					
Product: pricing_deals_for_woocommerce					
Affected Version(s): * Up to (including) 2.0.2.02					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Jul-2022	9.8	The Pricing Deals for WooCommerce WordPress plugin through 2.0.2.02 does not properly sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to an unauthenticated SQL injection **CVE ID : CVE-2022-1057**	N/A	A-VAR-PRIC-200722/514
Vendor: Vicidial					
Product: vicidial					
Affected Version(s): 2.14b0.5					
Improper Neutralization of Special Elements used in an SQL	05-Jul-2022	8.8	SQL Injection vulnerability in admin interface (/vicidial/admin.php) of VICIdial via modify_email_accounts, access_recordings,	https://www.vicidial.org/VICIDIALforum/viewtopic.php?f=4&t=41300&sid=aacb27a29fefd85265b4d55	A-VIC-VICI-200722/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			and agentcall_email parameters allows attacker to spoof identity, tamper with existing data, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server. This issue affects: VICIdial 2.14b0.5 versions prior to 3555. **CVE ID : CVE-2022-34876**	fe51122af, https://github.com/rapid7/metasploit-framework/pull/16732	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2022	8.8	SQL Injection vulnerability in AST Agent Time Sheet interface ((/vicidial/AST_agent_time_sheet.php) of VICIdial via the agent parameter allows attacker to spoof identity, tamper with existing data, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server. This issue affects: VICIdial 2.14b0.5 versions prior to 3555.	https://www.vicidial.org/VICIDIALforum/viewtopic.php?f=4&t=41300&sid=aacb27a29fefd85265b4d55fe51122af, https://github.com/rapid7/metasploit-framework/pull/16732	A-VIC-VICI-200722/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34877		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2022	8.8	SQL Injection vulnerability in User Stats interface (/vicidial/user_stats.php) of VICIdial via the file_download parameter allows attacker to spoof identity, tamper with existing data, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server. **CVE ID : CVE-2022-34878**	https://www.vicidial.org/VICIDIALforum/viewtopic.php?f=4&t=41300&sid=aacb27a29ffd85265b4d55fe51122af, https://github.com/rapid7/metasploit-framework/pull/16732	A-VIC-VICI-200722/517
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2022	6.1	Reflected Cross Site Scripting (XSS) vulnerabilities in AST Agent Time Sheet interface (/vicidial/AST_agent_time_sheet.php) of VICIdial via agent, and search_archived_data parameters. This issue affects: VICIdial 2.14b0.5 versions prior to 3555. **CVE ID : CVE-2022-34879**	https://www.vicidial.org/VICIDIALforum/viewtopic.php?f=4&t=41300&sid=aacb27a29ffd85265b4d55fe51122af	A-VIC-VICI-200722/518
Vendor: videoserver_project					
Product: videoserver					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2019-09-21					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The shaolo1/VideoServer repository through 2019-09-21 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31582**	N/A	A-VID-VIDE-200722/519
Vendor: VIM					
Product: vim					
Affected Version(s): * Up to (excluding) 9.0.0011					
Heap-based Buffer Overflow	01-Jul-2022	7.8	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0. **CVE ID : CVE-2022-2264**	https://github.com/vim/vim/commit/d25f003342aca9889067f2e839963dfeccf1fe05, https://huntr.dev/bounties/2241c773-02c9-4708-b63e-54aef99afa6c	A-VIM-VIM-200722/520
Affected Version(s): * Up to (excluding) 9.0.0017					
Heap-based Buffer Overflow	02-Jul-2022	7.8	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0. **CVE ID : CVE-2022-2284**	https://huntr.dev/bounties/571d25ce-8d53-4fa0-b620-27f2a8a14874, https://github.com/vim/vim/commit/3d51ce18ab1be4f9f6061568a4e7fabf00b21794	A-VIM-VIM-200722/521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 9.0.0018					
Integer Overflow or Wraparound	02-Jul-2022	7.8	Integer Overflow or Wraparound in GitHub repository vim/vim prior to 9.0. **CVE ID : CVE-2022-2285**	https://github.com/vim/vim/commit/27efc62f5d86afcb2ecb7565587fe8dea4b036fe, https://huntr.dev/bounties/64574b28-1779-458d-a221-06c434042736	A-VIM-VIM-200722/522
Affected Version(s): * Up to (excluding) 9.0.0020					
Out-of-bounds Read	02-Jul-2022	7.8	Out-of-bounds Read in GitHub repository vim/vim prior to 9.0. **CVE ID : CVE-2022-2286**	https://huntr.dev/bounties/fe7681fb-2318-436b-8e65-daf66cd597d8, https://github.com/vim/vim/commit/f12129f1714f7d2301935bb21d896609bdac221c	A-VIM-VIM-200722/523
Affected Version(s): * Up to (excluding) 9.0.0021					
Out-of-bounds Read	02-Jul-2022	7.1	Out-of-bounds Read in GitHub repository vim/vim prior to 9.0. **CVE ID : CVE-2022-2287**	https://github.com/vim/vim/commit/5e59ea54c0c37c2f84770f068d95280069828774, https://huntr.dev/bounties/654aa069-3a9d-45d3-9a52-c1cf3490c284	A-VIM-VIM-200722/524
Affected Version(s): * Up to (excluding) 9.0.0025					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Jul-2022	7.8	Out-of-bounds Write in GitHub repository vim/vim prior to 9.0. **CVE ID : CVE-2022-2288**	https://huntr.dev/bounties/a71bdcb7-4e9b-4650-ab6a-fe8e3e9852ad, https://github.com/vim/vim/commit/c6fdb15d423df22e1776844811d082322475e48a	A-VIM-VIM-200722/525
Affected Version(s): * Up to (excluding) 9.0.0026					
Use After Free	03-Jul-2022	7.8	Use After Free in GitHub repository vim/vim prior to 9.0. **CVE ID : CVE-2022-2289**	https://github.com/vim/vim/commit/c5274dd12224421f2430b30c53b881b9403d649e, https://huntr.dev/bounties/7447d2ea-db5b-4883-adf4-1eaf7deace64	A-VIM-VIM-200722/526
Affected Version(s): * Up to (excluding) 9.0.0035					
Stack-based Buffer Overflow	05-Jul-2022	7.8	Stack-based Buffer Overflow in GitHub repository vim/vim prior to 9.0. **CVE ID : CVE-2022-2304**	https://github.com/vim/vim/commit/54e5fed6d27b747ff152cdb6edfb72ff60e70939, https://huntr.dev/bounties/eb7402f3-025a-402f-97a7-c38700d9548a	A-VIM-VIM-200722/527
Affected Version(s): * Up to (excluding) 9.0.0045					
Heap-based	08-Jul-2022	7.8	Heap-based Buffer Overflow in GitHub	https://github.com/vim/vim/commit/baefde	A-VIM-VIM-200722/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			repository vim/vim prior to 9.0.0045. **CVE ID : CVE-2022-2344**	14550231f6468ac2ed2ed495bc381c0c92, https://huntr.dev/bounties/4a095ed9-3125-464a-b656-c31b437e1996	
Affected Version(s): * Up to (excluding) 9.0.0046					
Use After Free	08-Jul-2022	7.8	Use After Free in GitHub repository vim/vim prior to 9.0.0046. **CVE ID : CVE-2022-2345**	https://huntr.dev/bounties/1eed7009-db6d-487b-bc41-8f2fd260483f, https://github.com/vim/vim/commit/32acf1f1a72ebb9d8942b9c9d80023bf1bb668ea	A-VIM-VIM-200722/529
Vendor: visser					
Product: woocommerce_-_product_importer					
Affected Version(s): * Up to (including) 1.5.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2022	6.1	The WooCommerce - Product Importer WordPress plugin through 1.5.2 does not sanitise and escape the imported data before outputting it back in the page, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-1546**	N/A	A-VIS-WOOC-200722/530
Vendor: Vmware					
Product: vrealize_log_insight					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 8.8.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-2022	5.4	VMware vRealize Log Insight in versions prior to 8.8.2 contain a stored cross-site scripting vulnerability due to improper input sanitization in configurations. **CVE ID : CVE-2022-31654**	https://www.vmware.com/security/advisories/VMSA-2022-0019.html	A-VMW-VREA-200722/531
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-2022	5.4	VMware vRealize Log Insight in versions prior to 8.8.2 contain a stored cross-site scripting vulnerability due to improper input sanitization in alerts. **CVE ID : CVE-2022-31655**	https://www.vmware.com/security/advisories/VMSA-2022-0019.html	A-VMW-VREA-200722/532
Vendor: vprj_project					
Product: vprj					
Affected Version(s): * Up to (including) 2022-04-06					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The whmacmac/vprj repository through 2022-04-06 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31563**	N/A	A-VPR-VPRJ-200722/533
Vendor: webswing					
Product: webswing					
Affected Version(s): * Up to (excluding) 20.1.16					
Improper Neutralizat	08-Jul-2022	9.8	Webswing before 22.1.3 allows X-	https://www.webswing.org/	A-WEB-WEBS-200722/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements in Output Used by a Downstream Component ('Injection')			Forwarded-For header injection. The client IP address is associated with a variable in the configuration page. The {clientIp} variable can be used as an application startup argument. The X-Forwarded-For header can be manipulated by a client to store an arbitrary value that is used to replace the clientIp variable (without sanitization). A client can thus inject multiple arguments into the session startup. Systems that do not use the clientIP variable in the configuration are not vulnerable. The vulnerability is fixed in these versions: 20.1.16, 20.2.19, 21.1.8, 21.2.12, and 22.1.3. **CVE ID : CVE-2022-34914**	docs/20.1/faq/client_ip.html, https://www.webswing.org/blog/header-injection-vulnerability-cve-2022-34914	
Affected Version(s): From (including) 20.2 Up to (excluding) 20.2.19					
Improper Neutralization of Special Elements in Output Used by a Downstrea	08-Jul-2022	9.8	Webswing before 22.1.3 allows X-Forwarded-For header injection. The client IP address is associated with a variable in the configuration page.	https://www.webswing.org/docs/20.1/faq/client_ip.html, https://www.webswing.org/blog/header-injection-	A-WEB-WEBS-200722/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')			The {clientIp} variable can be used as an application startup argument. The X-Forwarded-For header can be manipulated by a client to store an arbitrary value that is used to replace the clientIp variable (without sanitization). A client can thus inject multiple arguments into the session startup. Systems that do not use the clientIP variable in the configuration are not vulnerable. The vulnerability is fixed in these versions: 20.1.16, 20.2.19, 21.1.8, 21.2.12, and 22.1.3. **CVE ID : CVE-2022-34914**	vulnerability-cve-2022-34914	
Affected Version(s): From (including) 21.1.0 Up to (excluding) 21.1.8					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Jul-2022	9.8	Webswing before 22.1.3 allows X-Forwarded-For header injection. The client IP address is associated with a variable in the configuration page. The {clientIp} variable can be used as an application startup argument. The X-Forwarded-For header can be	https://www.webswing.org/docs/20.1/faq/client_ip.html, https://www.webswing.org/blog/header-injection-vulnerability-cve-2022-34914	A-WEB-WEBS-200722/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulated by a client to store an arbitrary value that is used to replace the clientIp variable (without sanitization). A client can thus inject multiple arguments into the session startup. Systems that do not use the clientIP variable in the configuration are not vulnerable. The vulnerability is fixed in these versions: 20.1.16, 20.2.19, 21.1.8, 21.2.12, and 22.1.3. **CVE ID : CVE-2022-34914**		
Affected Version(s): From (including) 21.2.0 Up to (excluding) 21.2.12					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Jul-2022	9.8	Webswing before 22.1.3 allows X-Forwarded-For header injection. The client IP address is associated with a variable in the configuration page. The {clientIp} variable can be used as an application startup argument. The X-Forwarded-For header can be manipulated by a client to store an arbitrary value that is used to replace the clientIp variable (without	https://www.webswing.org/docs/20.1/faq/client_ip.html, https://www.webswing.org/blog/header-injection-vulnerability-cve-2022-34914	A-WEB-WEBS-200722/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sanitization). A client can thus inject multiple arguments into the session startup. Systems that do not use the clientIP variable in the configuration are not vulnerable. The vulnerability is fixed in these versions: 20.1.16, 20.2.19, 21.1.8, 21.2.12, and 22.1.3. **CVE ID : CVE-2022-34914**		
Affected Version(s): From (including) 22.1.0 Up to (excluding) 22.1.3					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Jul-2022	9.8	Webswing before 22.1.3 allows X-Forwarded-For header injection. The client IP address is associated with a variable in the configuration page. The {clientIp} variable can be used as an application startup argument. The X-Forwarded-For header can be manipulated by a client to store an arbitrary value that is used to replace the clientIp variable (without sanitization). A client can thus inject multiple arguments into the session startup. Systems that do not use the	https://www.webswing.org/docs/20.1/faq/client_ip.html, https://www.webswing.org/blog/header-injection-vulnerability-cve-2022-34914	A-WEB-WEBS-200722/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clientIP variable in the configuration are not vulnerable. The vulnerability is fixed in these versions: 20.1.16, 20.2.19, 21.1.8, 21.2.12, and 22.1.3. **CVE ID : CVE-2022-34914**		
Vendor: windmill_project					
Product: windmill					
Affected Version(s): 1.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The Lukasavicus/WindMill repository through 1.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31519**	N/A	A-WIN-WIND-200722/539
Vendor: withknown					
Product: known					
Affected Version(s): * Up to (including) 1.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2022	6.1	An issue in the isSVG() function of Known v1.2.2+2020061101 allows attackers to execute arbitrary code via a crafted SVG file. **CVE ID : CVE-2022-32115**	https://withknown.com/	A-WIT-KNOW-200722/540
Improper Neutralization of	08-Jul-2022	5.4	A cross-site scripting (XSS) vulnerability in Known	https://withknown.com/, http://docs.wit	A-WIT-KNOW-200722/541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			v1.2.2+2020061101 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Your Name text field. **CVE ID : CVE-2022-31290**	hknown.com/en/latest/install/index.html	
Authorization Bypass Through User-Controlled Key	08-Jul-2022	4.3	Known v1.3.1 was discovered to contain an Insecure Direct Object Reference (IDOR). **CVE ID : CVE-2022-30852**	https://withknown.com/, https://blog.jitendrapatro.me/multiple-vulnerabilities-in-idno-known-php-cms-software/	A-WIT-KNOW-200722/542
Vendor: wormnest_project					
Product: wormnest					
Affected Version(s): * Up to (including) 0.4.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The operatorequals/wormnest repository through 0.4.7 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31502**	https://github.com/operatorequals/wormnest/commit/2dfe96fc2570586ac487b399ac20d41b3c114861	A-WOR-WORM-200722/543
Vendor: wp-championship_project					
Product: wp-championship					
Affected Version(s): * Up to (excluding) 9.3					
Cross-Site Request	04-Jul-2022	6.5	The WP Championship WordPress plugin	N/A	A-WP--WP-C-200722/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			before 9.3 is lacking CSRF checks in various places, allowing attackers to make a logged in admin perform unwanted actions, such as create and delete arbitrary teams as well as update the plugin's settings. Due to the lack of sanitisation and escaping, it could also lead to Stored Cross-Site Scripting issues **CVE ID : CVE-2022-1967**		
Vendor: wp-eventmanager					
Product: wp_event_manager					
Affected Version(s): * Up to (excluding) 3.1.28					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2022	6.1	The WP Event Manager WordPress plugin before 3.1.28 does not sanitise and escape its search before outputting it back in an attribute on the event dashboard, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-1474**	N/A	A-WP--WP_E-200722/545
Vendor: wpdevart					
Product: gallery					
Affected Version(s): * Up to (excluding) 2.0.0					
Improper Neutralization of	04-Jul-2022	6.1	The Gallery WordPress plugin before 2.0.0 does not	N/A	A-WPD-GALL-200722/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			sanitise and escape a parameter before outputting it back in the response of an AJAX action (available to both unauthenticated and authenticated users), leading to a Reflected Cross-Site Scripting issue **CVE ID : CVE-2022-1946**		
Vendor: wpexperts					
Product: wp_contact_slider					
Affected Version(s): * Up to (excluding) 2.4.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jul-2022	4.8	The WP Contact Slider WordPress plugin before 2.4.7 does not sanitize and escape the Text to Display settings of sliders, which could allow high privileged users such as editor and above to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed **CVE ID : CVE-2022-1301**	N/A	A-WPE-WP_C-200722/547
Vendor: wp_opt-in_project					
Product: wp_opt-in					
Affected Version(s): * Up to (including) 1.4.1					
Cross-Site Request Forgery (CSRF)	11-Jul-2022	4.3	The WP Opt-in WordPress plugin through 1.4.1 is vulnerable to CSRF which allows changed plugin settings and	N/A	A-WP_-WP_O-200722/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can be used for sending spam emails. **CVE ID : CVE-2022-2123**		
Vendor: xgenecloud					
Product: nocodb					
Affected Version(s): * Up to (excluding) 0.92.0					
Server-Side Request Forgery (SSRF)	07-Jul-2022	7.5	With this SSRF vulnerability, an attacker can reach internal addresses to make a request as the server and read it's contents. This attack can lead to leak of sensitive information. **CVE ID : CVE-2022-2339**	https://huntr.dev/bounties/fff06de8-2a82-49b1-8e81-968731e87eef, https://github.com/nocodb/nocodb/commit/000ecd886738b965b5997cd905825e3244f48b95	A-XGE-NOCO-200722/549
Vendor: Xmlsoft					
Product: libxml2					
Affected Version(s): From (including) 2.9.10 Up to (including) 2.9.14					
NULL Pointer Dereference	05-Jul-2022	7.5	NULL Pointer Dereference allows attackers to cause a denial of service (or application crash). This only applies when lxml is used together with libxml2 2.9.10 through 2.9.14. libxml2 2.9.9 and earlier are not affected. It allows triggering crashes through forged input data, given a vulnerable code sequence in the application. The vulnerability is	https://huntr.dev/bounties/8264e74f-edda-4c40-9956-49de635105ba, https://github.com/lxml/lxml/commit/86368e9cf70a0ad23cccd5ee32de847149af0c6f	A-XML-LIBX-200722/550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			caused by the iterwalk function (also used by the canonicalize function). Such code shouldn't be in wide-spread use, given that parsing + iterwalk would usually be replaced with the more efficient iterparse function. However, an XML converter that serialises to C14N would also be vulnerable, for example, and there are legitimate use cases for this code sequence. If untrusted input is received (also remotely) and processed via iterwalk function, a crash can be triggered. **CVE ID : CVE-2022-2309**		
Vendor: xtomo					
Product: robo-tom					
Affected Version(s): * Up to (including) 1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The meerstein/rbtm repository through 1.5 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31544**	N/A	A-XTO-ROBO-200722/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: ytdl-sync_project					
Product: ytdl-sync					
Affected Version(s): * Up to (including) 2021-01-02					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2022	9.3	The jaygarza1982/ytdl-sync repository through 2021-01-02 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. **CVE ID : CVE-2022-31536**	N/A	A-YTD-YTDL-200722/552
Vendor: Zabbix					
Product: Zabbix					
Affected Version(s): * Up to (excluding) 4.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2022	5.4	An authenticated user can create a link with reflected Javascript code inside it for the discovery page and send it to other users. The payload can be executed only with a known CSRF token value of the victim, which is changed periodically and is difficult to predict. **CVE ID : CVE-2022-35229**	https://support.zabbix.com/browse/ZBX-21306	A-ZAB-ZABB-200722/553
Affected Version(s): * Up to (excluding) 5.0.25					
Improper Neutralization of Input During Web Page	06-Jul-2022	5.4	An authenticated user can create a link with reflected Javascript code inside it for the graphs page and send it to other users. The	https://support.zabbix.com/browse/ZBX-21305	A-ZAB-ZABB-200722/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			payload can be executed only with a known CSRF token value of the victim, which is changed periodically and is difficult to predict. **CVE ID : CVE-2022-35230**		
Affected Version(s): 5.0.25					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2022	5.4	An authenticated user can create a link with reflected Javascript code inside it for the discovery page and send it to other users. The payload can be executed only with a known CSRF token value of the victim, which is changed periodically and is difficult to predict. **CVE ID : CVE-2022-35229**	https://support.zabbix.com/browse/ZBX-21306	A-ZAB-ZABB-200722/555
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2022	5.4	An authenticated user can create a link with reflected Javascript code inside it for the graphs page and send it to other users. The payload can be executed only with a known CSRF token value of the victim, which is changed periodically and is difficult to predict. **CVE ID : CVE-2022-35230**	https://support.zabbix.com/browse/ZBX-21305	A-ZAB-ZABB-200722/556
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.0.25					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2022	5.4	An authenticated user can create a link with reflected Javascript code inside it for the discovery page and send it to other users. The payload can be executed only with a known CSRF token value of the victim, which is changed periodically and is difficult to predict. **CVE ID : CVE-2022-35229**	https://support.zabbix.com/browse/ZBX-21306	A-ZAB-ZABB-200722/557
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2022	5.4	An authenticated user can create a link with reflected Javascript code inside it for the discovery page and send it to other users. The payload can be executed only with a known CSRF token value of the victim, which is changed periodically and is difficult to predict. **CVE ID : CVE-2022-35229**	https://support.zabbix.com/browse/ZBX-21306	A-ZAB-ZABB-200722/558
Vendor: Zimbra					
Product: collaboration					
Affected Version(s): 8.8.15					
Incorrect Authorization	11-Jul-2022	9.8	Zimbra Collaboration Open Source 8.8.15 does not encrypt the initial-login randomly created password (from the "zmproveca" command). It is	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories, https://wiki.zimbra.com/wik	A-ZIM-COLL-200722/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			visible in cleartext on port UDP 514 (aka the syslog port). **CVE ID : CVE-2022-32294**	i/Security_Center	
Vendor: Zohocorp					
Product: manageengine_adselfservice_plus					
Affected Version(s): * Up to (excluding) 6.2					
N/A	04-Jul-2022	7.5	Zoho ManageEngine ADSelfService Plus before 6203 allows a denial of service (application restart) via a crafted payload to the Mobile App Deployment API. **CVE ID : CVE-2022-34829**	https://www.manageengine.com/products/self-service-password/advisory/CVE-2022-34829.html	A-ZOH-MANA-200722/560
Affected Version(s): 6.2					
N/A	04-Jul-2022	7.5	Zoho ManageEngine ADSelfService Plus before 6203 allows a denial of service (application restart) via a crafted payload to the Mobile App Deployment API. **CVE ID : CVE-2022-34829**	https://www.manageengine.com/products/self-service-password/advisory/CVE-2022-34829.html	A-ZOH-MANA-200722/561
Product: manageengine_servicedesk_plus_msp					
Affected Version(s): * Up to (excluding) 10.6					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Jul-2022	7.5	Zoho ManageEngine ServiceDesk Plus MSP before 10604 allows path traversal (to WEBINF/web.xml from sample/WEB-INF/web.xml or sample/META-INF/web.xml).	https://www.manageengine.com/products/service-desk-msp/CVE-2022-32551.html	A-ZOH-MANA-200722/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32551		
Affected Version(s): 10.6					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Jul-2022	7.5	Zoho ManageEngine ServiceDesk Plus MSP before 10604 allows path traversal (to WEBINF/web.xml from sample/WEB-INF/web.xml or sample/META-INF/web.xml). **CVE ID : CVE-2022-32551**	https://www.manageengine.com/products/service-desk-msp/CVE-2022-32551.html	A-ZOH-MANA-200722/563
Vendor: zoo_management_system_project					
Product: zoo_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2022	5.4	A stored cross-site scripting (XSS) vulnerability in the Add Classification function of Zoo Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via unspecified vectors. **CVE ID : CVE-2022-33075**	N/A	A-ZOO-ZOO_-200722/564
Hardware					
Vendor: amperecomputing					
Product: ampere_altra					
Affected Version(s): -					
Incorrect Authorization	01-Jul-2022	9.8	On Ampere Altra and AltraMax devices before SRP 1.09, the the Altra reference design of UEFI	https://amperecomputing.com	H-AMP-AMPE-200722/565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accesses allows insecure access to SPI-NOR by the OS/hypervisor component. **CVE ID : CVE-2022-32295**		
Product: ampere_altra_max					
Affected Version(s): -					
Incorrect Authorization	01-Jul-2022	9.8	On Ampere Altra and AltraMax devices before SRP 1.09, the the Altra reference design of UEFI accesses allows insecure access to SPI-NOR by the OS/hypervisor component. **CVE ID : CVE-2022-32295**	https://amperecomputing.com	H-AMP-AMPE-200722/566
Vendor: Asus					
Product: dsl-n14u-b1					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jul-2022	5.4	Cross Site Scripting (XSS) vulnerability in router Asus DSL-N14U-B1 1.1.2.3_805 via the "*list" parameters (e.g. filter_lwlist, keyword_rulelist, etc) in every ".asp" page containing a list of stored strings. The following asp files are affected: (1) cgi-bin/APP_Installation.asp, (2) cgi-bin/Advanced_ACL_Content.asp, (3) cgi-	N/A	H-ASU-DSL--200722/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/Advanced_ADSL_Content.asp, (4) cgi-bin/Advanced_ASUSDDNS_Content.asp, (5) cgi-bin/Advanced_AiDisk_ftp.asp, (6) cgi-bin/Advanced_AiDisk_samba.asp, (7) cgi-bin/Advanced_DSL_Content.asp, (8) cgi-bin/Advanced_Firewall_Content.asp, (9) cgi-bin/Advanced_FirmwareUpgrade_Content.asp, (10) cgi-bin/Advanced_GWStaticRoute_Content.asp, (11) cgi-bin/Advanced_IPTV_Content.asp, (12) cgi-bin/Advanced_IPv6_Content.asp, (13) cgi-bin/Advanced_KeywordFilter_Content.asp, (14) cgi-bin/Advanced_LAN_Content.asp, (15) cgi-bin/Advanced_Modem_Content.asp, (16) cgi-bin/Advanced_PortTrigger_Content.asp, (17) cgi-bin/Advanced_QOSUserPrio_Content.asp, (18) cgi-bin/Advanced_QOSUserRules_Content.asp, (19) cgi-bin/Advanced_SettingBackup_Content.asp, (20) cgi-bin/Advanced_Syste		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			m_Content.asp, (21) cgi-bin/Advanced_URLFilter_Content.asp, (22) cgi-bin/Advanced_VPN_PPTP.asp, (23) cgi-bin/Advanced_VirtualServer_Content.asp, (24) cgi-bin/Advanced_WANPort_Content.asp, (25) cgi-bin/Advanced_WAdvanced_Content.asp, (26) cgi-bin/Advanced_WMode_Content.asp, (27) cgi-bin/Advanced_WWPS_Content.asp, (28) cgi-bin/Advanced_Wireless_Content.asp, (29) cgi-bin/Bandwidth_Limiter.asp, (30) cgi-bin/Guest_network.asp, (31) cgi-bin/Main_AccessLog_Content.asp, (32) cgi-bin/Main_AdslStatus_Content.asp, (33) cgi-bin/Main_Spectrum_Content.asp, (34) cgi-bin/Main_WebHistory_Content.asp, (35) cgi-bin/ParentalControl.asp, (36) cgi-bin/QIS_wizard.asp, (37) cgi-bin/QoS_EZQoS.asp, (38) cgi-bin/aidisk.asp, (39)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cgi-bin/aidisk/Aidisk-1.asp, (40) cgi-bin/aidisk/Aidisk-2.asp, (41) cgi-bin/aidisk/Aidisk-3.asp, (42) cgi-bin/aidisk/Aidisk-4.asp, (43) cgi-bin/blocking.asp, (44) cgi-bin/cloud_main.asp, (45) cgi-bin/cloud_router_sync.asp, (46) cgi-bin/cloud_settings.asp, (47) cgi-bin/cloud_sync.asp, (48) cgi-bin/device-map/DSL_dashboard.asp, (49) cgi-bin/device-map/clients.asp, (50) cgi-bin/device-map/disk.asp, (51) cgi-bin/device-map/internet.asp, (52) cgi-bin/error_page.asp, (53) cgi-bin/index.asp, (54) cgi-bin/index2.asp, (55) cgi-bin/qis/QIS_PTM_manual_setting.asp, (56) cgi-bin/qis/QIS_admin_pass.asp, (57) cgi-bin/qis/QIS_annex_setting.asp, (58) cgi-bin/qis/QIS_bridge_cfg_tmp.asp, (59) cgi-bin/qis/QIS_detect.asp, (60) cgi-bin/qis/QIS_finish.as		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			p, (61) cgi-bin/qis/QIS_ipoa_cfg_tmp.asp, (62) cgi-bin/qis/QIS_manual_setting.asp, (63) cgi-bin/qis/QIS_mer_cfg.asp, (64) cgi-bin/qis/QIS_mer_cfg_tmp.asp, (65) cgi-bin/qis/QIS_ppp_cfg.asp, (66) cgi-bin/qis/QIS_ppp_cfg_tmp.asp, (67) cgi-bin/qis/QIS_wireless.asp, (68) cgi-bin/query_wan_status.asp, (69) cgi-bin/query_wan_status2.asp, and (70) cgi-bin/start_apply.asp. **CVE ID : CVE-2022-32988**		
Vendor: gallagher					
Product: controller_6000					
Affected Version(s): -					
N/A	06-Jul-2022	7.5	Gallagher Controller 6000 is vulnerable to a Denial of Service attack via conflicting ARP packets with a duplicate IP address. This issue affects: Gallagher Gallagher Controller 6000 vCR8.60 versions prior to 220303a; vCR8.50 versions prior to 220303a; vCR8.40 versions prior to 220303a; vCR8.30 versions prior to 220303a.	https://security.gallagher.com/Security-Advisories/CVE-2022-26078	H-GAL-CONT-200722/568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26078		
Vendor: H3C					
Product: magic_r100					
Affected Version(s): -					
N/A	06-Jul-2022	9.8	The udpserver in H3C Magic R100 V200R004 and V100R005 has the 9034 port opened, allowing attackers to execute arbitrary commands. **CVE ID : CVE-2022-34598**	N/A	H-H3C-MAGI-200722/569
Vendor: hpe					
Product: flexfabric_5945					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2022	4.8	A potential security vulnerability has been identified in certain HPE FlexNetwork and FlexFabric switch products. The vulnerability could be remotely exploited to allow cross site scripting (XSS). HPE has made the following software updates to resolve the vulnerability. HPE FlexNetwork 5130EL_7.10.R3507P02 and HPE FlexFabric 5945_7.10.R6635. **CVE ID : CVE-2022-28624**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04265en_us	H-HPE-FLEX-200722/570
Product: flexnetwork_5130_ei					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2022	4.8	A potential security vulnerability has been identified in certain HPE FlexNetwork and FlexFabric switch products. The vulnerability could be remotely exploited to allow cross site scripting (XSS). HPE has made the following software updates to resolve the vulnerability. HPE FlexNetwork 5130EL_7.10.R3507P02 and HPE FlexFabric 5945_7.10.R6635. **CVE ID : CVE-2022-28624**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04265en_us	H-HPE-FLEX-200722/571
Vendor: Kddi					
Product: home_spot_cube_2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Jul-2022	8.8	HOME SPOT CUBE2 V102 contains an OS command injection vulnerability due to improper processing of data received from DHCP server. An adjacent attacker may execute an arbitrary OS command on the product if a malicious DHCP server is placed on the WAN side of the product. **CVE ID : CVE-2022-33948**	https://www.au.com/support/service/mobile/guide/wlan/home_spot_cube_2/	H-KDD-HOME-200722/572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: mediatek					
Product: mt2601					
Affected Version(s): -					
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT26-200722/573
Product: mt2731					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT27-200722/574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT27-200722/575
Product: mt2735					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT27-200722/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20083		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT27-200722/577
Product: mt6297					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883;	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT62-200722/578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT62-200722/579
Product: mt6580					
Affected Version(s): -					
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT65-200722/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21777		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT65-200722/581
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT65-200722/582
Concurrent Execution using Shared Resource with Improper Synchroniz	06-Jul-2022	6.7	In GED driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT65-200722/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			needed. User interaction is not needed for exploitation. Patch ID: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT65-200722/584
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT65-200722/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT65-200722/586
Product: mt6725					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/587
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT67-200722/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	bulletin/July-2022	
Product: mt6735					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/589
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-200722/590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	bulletin/July-2022	
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/591
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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/July-2022	H-MED-MT67-200722/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/593
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/594
Concurrent Execution using	06-Jul-2022	6.7	In TEEI driver, there is a possible use after free due to a race	https://corp.mediatek.com/product-	H-MED-MT67-200722/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	security-bulletin/July-2022	
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/596
Product: mt6737					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/598
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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/July-2022	H-MED-MT67-200722/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/600
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/601
Concurrent Execution using Shared Resource with	06-Jul-2022	6.7	In TEEI driver, 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-bulletin/July-2022	H-MED-MT67-200722/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**		
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/603
Product: mt6739					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/605
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21777		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/607
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/608
Concurrent Execution using Shared Resource with Improper Synchroniz	06-Jul-2022	6.7	In GED driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			needed. User interaction is not needed for exploitation. Patch ID: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/610
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/612
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/613
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**		
Product: mt6750					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/615
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/617
Product: mt6750s					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883;	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/619
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt6753					
Affected Version(s): -					
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/621
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/622
Concurrent Execution using Shared Resource with Improper Synchroniz	06-Jul-2022	6.7	In GED driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			needed. User interaction is not needed for exploitation. Patch ID: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**		
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/624
Product: mt6755					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883;	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/626
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt6755s					
Affected Version(s): -					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/628
Product: mt6757					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/630
Product: mt6757p					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20083		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/632
Product: mt6758					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883;	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/634
Product: mt6761					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/636
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21777		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/638
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/639
Concurrent Execution using Shared Resource with Improper Synchroniz	06-Jul-2022	6.7	In GED driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			needed. User interaction is not needed for exploitation. Patch ID: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/641
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/642
Concurrent Execution	06-Jul-2022	6.7	In TEEI driver, there is a possible use after	https://corp.mediatek.com/p	H-MED-MT67-200722/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	roduct-security-bulletin/July-2022	
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/644
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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/July-2022	H-MED-MT67-200722/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/646
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/647
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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-bulletin/July-2022	H-MED-MT67-200722/648

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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/649
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/651
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/652
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**		
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/654
Product: mt6762					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20083		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/656
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/657
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after	https://corp.mediatek.com/p	H-MED-MT67-200722/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	roduct-security-bulletin/July-2022	
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/659
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**		
Product: mt6762d					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/661
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Product: mt6762m					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/663
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Product: mt6763					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/665
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/667
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/669
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/670
Product: mt6765					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/672
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/674
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/675
Concurrent Execution	06-Jul-2022	6.7	In GED driver, there is a possible use after	https://corp.mediatek.com/p	H-MED-MT67-200722/676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	roduct-security-bulletin/July-2022	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/677
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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/July-2022	H-MED-MT67-200722/678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/679
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/680
Concurrent Execution using Shared Resource with	06-Jul-2022	6.4	In MDP, 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-bulletin/July-2022	H-MED-MT67-200722/681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/682
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21764		
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/684
Product: mt6765t					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/686
Product: mt6767					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20083		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/688
Product: mt6768					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883;	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/690
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/692
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/693
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/695
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/696
Concurrent Execution using Shared Resource	06-Jul-2022	6.7	In TEEI driver, 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-MT67-200722/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	bulletin/July-2022	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/698
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21775		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/700
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/701
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**		
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/703
Product: mt6769					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/705
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20082		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/707
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/708
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/710
Product: mt6769t					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/712
Product: mt6769z					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/714
Product: mt6771					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/716
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/718
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/719
Concurrent Execution using Shared Resource with	06-Jul-2022	6.7	In GED driver, 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-bulletin/July-2022	H-MED-MT67-200722/720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/721
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/723
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/724
Concurrent Execution using Shared Resource with Improper Synchronization	06-Jul-2022	6.4	In MDP, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			exploitation. Patch ID: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/726
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/727
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, there is a possible out of bounds read due to a	https://corp.mediatek.com/product-	H-MED-MT67-200722/728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	security-bulletin/July-2022	
Product: mt6775					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/729
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Product: mt6779					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/731
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/733
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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/July-2022	H-MED-MT67-200722/734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/735
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/736
Concurrent Execution using Shared Resource with	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion due to a race condition. This could lead to local escalation of privilege	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/738
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/740
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/741
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/743
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/744
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT67-200722/745

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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	bulletin/July-2022	
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/746
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21776		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/748
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/749
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**		
Product: mt6781					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/751
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/753
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21765		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/755
Improper Link Resolution Before File Access ('Link Following')	06-Jul-2022	6.7	In sound driver, there is a possible information disclosure due to symlink following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558663; Issue ID: ALPS06558663. **CVE ID : CVE-2022-21770**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/756
Concurrent Execution using Shared Resource with Improper	06-Jul-2022	6.7	In GED driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/758
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/760
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/761
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/763
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/764
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT67-200722/765

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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	bulletin/July-2022	
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/766
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21776		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/768
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/769
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**		
Product: mt6783					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/771
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Product: mt6785					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/773
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/775
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20082		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/777
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/778
Concurrent Execution using Shared Resource with Improper Synchroniz	06-Jul-2022	6.7	In GED driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			needed. User interaction is not needed for exploitation. Patch ID: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/780
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/781
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after	https://corp.mediatek.com/p	H-MED-MT67-200722/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	roduct-security-bulletin/July-2022	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/783
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/785
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/786
Product: mt6785t					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/787
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/788
Product: mt6789					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/789
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/791
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/792
Concurrent Execution using Shared Resource with Improper Synchronization	06-Jul-2022	6.7	In TEEI driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			exploitation. Patch ID: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**		
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/794
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/795
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission	https://corp.mediatek.com/product-security-	H-MED-MT67-200722/796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	bulletin/July-2022	
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/797
Product: mt6795					
Affected Version(s): -					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**		
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/799
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/800
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a	https://corp.mediatek.com/product-security-	H-MED-MT67-200722/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	bulletin/July-2022	
Product: mt6797					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/802
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/804
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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/July-2022	H-MED-MT67-200722/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/806
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/807
Product: mt6799					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/808
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/810
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/811
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT67-200722/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**		
Product: mt6833					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/813
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/815
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/817
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/818
Concurrent Execution using Shared Resource with Improper Synchronization	06-Jul-2022	6.7	In GED driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			exploitation. Patch ID: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/820
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/821
Concurrent Execution using Shared Resource	06-Jul-2022	6.7	In TEEI driver, 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-MT68-200722/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	bulletin/July-2022	
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/823
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21779		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/825
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/826
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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/July-2022	H-MED-MT68-200722/827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/828
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/829
Incorrect Type	06-Jul-2022	6.7	In audio DSP, there is a possible memory	https://corp.mediatek.com/p	H-MED-MT68-200722/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			corruption due to improper casting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558822; Issue ID: ALPS06558822. **CVE ID : CVE-2022-21786**	roduct-security-bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	6.7	In audio DSP, 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: ALPS06558844; Issue ID: ALPS06558844. **CVE ID : CVE-2022-21787**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/831
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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/July-2022	H-MED-MT68-200722/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/833
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/834
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-200722/835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	bulletin/July-2022	
Product: mt6853					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/836
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/838
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/840
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/841
Concurrent Execution using Shared Resource with	06-Jul-2022	6.7	In GED driver, 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-bulletin/July-2022	H-MED-MT68-200722/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/843
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/845
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/846
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/848
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/849
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT68-200722/850

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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	bulletin/July-2022	
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/851
Incorrect Type Conversion or Cast	06-Jul-2022	6.7	In audio DSP, there is a possible memory corruption due to improper casting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558822; Issue ID: ALPS06558822.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21786		
Out-of-bounds Write	06-Jul-2022	6.7	In audio DSP, 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: ALPS06558844; Issue ID: ALPS06558844. **CVE ID : CVE-2022-21787**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/853
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/854
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/856
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt6853t					
Affected Version(s): -					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/858
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/859
Concurrent Execution using Shared Resource with Improper Synchroniz	06-Jul-2022	6.7	In TEEI driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			needed. User interaction is not needed for exploitation. Patch ID: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**		
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/861
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/863
Product: mt6855					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/864
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-200722/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	bulletin/July-2022	
Product: mt6873					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/866
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due	https://corp.mediatek.com/product-	H-MED-MT68-200722/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	security-bulletin/July-2022	
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/868
Concurrent Execution using Shared Resource with Improper Synchroniz	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/870
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/871
Concurrent Execution	06-Jul-2022	6.7	In GED driver, there is a possible use after	https://corp.mediatek.com/p	H-MED-MT68-200722/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	roduct-security-bulletin/July-2022	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/873
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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/July-2022	H-MED-MT68-200722/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/875
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/876
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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-bulletin/July-2022	H-MED-MT68-200722/877

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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/878
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/880
Incorrect Type Conversion or Cast	06-Jul-2022	6.7	In audio DSP, there is a possible memory corruption due to improper casting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558822; Issue ID: ALPS06558822. **CVE ID : CVE-2022-21786**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/881
Out-of-bounds Write	06-Jul-2022	6.7	In audio DSP, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06558844; Issue ID: ALPS06558844. **CVE ID : CVE-2022-21787**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/883
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/884
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a	https://corp.mediatek.com/product-security-	H-MED-MT68-200722/885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	bulletin/July-2022	
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/886
Product: mt6875					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/888
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/890
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/891
Concurrent Execution using Shared Resource with	06-Jul-2022	6.7	In TEEI driver, 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-bulletin/July-2022	H-MED-MT68-200722/892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**		
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/893
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21763		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/895
Product: mt6877					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/897
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/898
Concurrent Execution using Shared Resource	06-Jul-2022	7	In GPU, 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-MT68-200722/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**	bulletin/July-2022	
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/900
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21766		
Improper Link Resolution Before File Access ('Link Following')	06-Jul-2022	6.7	In sound driver, there is a possible information disclosure due to symlink following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558663; Issue ID: ALPS06558663. **CVE ID : CVE-2022-21770**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/902
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/903
Concurrent Execution using Shared Resource with Improper	06-Jul-2022	6.7	In TEEI driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/905
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/907
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/908
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/910
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/911
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT68-200722/912

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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/913
Incorrect Type Conversion or Cast	06-Jul-2022	6.7	In audio DSP, there is a possible memory corruption due to improper casting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558822; Issue ID: ALPS06558822.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21786		
Out-of-bounds Write	06-Jul-2022	6.7	In audio DSP, 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: ALPS06558844; Issue ID: ALPS06558844. **CVE ID : CVE-2022-21787**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/915
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/916
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/918
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt6879					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/920
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21744		
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/922
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/923
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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/July-2022	H-MED-MT68-200722/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/925
Improper Link Resolution Before File Access ('Link Following')	06-Jul-2022	6.7	In sound driver, there is a possible information disclosure due to symlink following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558663; Issue ID: ALPS06558663. **CVE ID : CVE-2022-21770**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/927
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/928
Concurrent Execution using Shared Resource with Improper Synchronization	06-Jul-2022	6.7	In TEEI driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			exploitation. Patch ID: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/930
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/931
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT68-200722/932

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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/933
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21781		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/935
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/936
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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/July-2022	H-MED-MT68-200722/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**		
Incorrect Type Conversion or Cast	06-Jul-2022	6.7	In audio DSP, there is a possible memory corruption due to improper casting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558822; Issue ID: ALPS06558822. **CVE ID : CVE-2022-21786**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/938
Out-of-bounds Write	06-Jul-2022	6.7	In audio DSP, 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: ALPS06558844; Issue ID: ALPS06558844. **CVE ID : CVE-2022-21787**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/939
Concurrent Execution	06-Jul-2022	6.4	In MDP, there is a possible use after free	https://corp.mediatek.com/p	H-MED-MT68-200722/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	roduct-security-bulletin/July-2022	
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/941
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**		
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/943
Product: mt6880					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20083		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/945
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/947
Product: mt6883					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/948
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-200722/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	bulletin/July-2022	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/950
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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/July-2022	H-MED-MT68-200722/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/952
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/953
Concurrent Execution using	06-Jul-2022	6.7	In TEEI driver, there is a possible use after free due to a race	https://corp.mediatek.com/product-	H-MED-MT68-200722/954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	security-bulletin/July-2022	
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/955
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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/July-2022	H-MED-MT68-200722/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/957
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/958
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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-bulletin/July-2022	H-MED-MT68-200722/959

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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/960
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/962
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/963
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**		
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/965
Product: mt6885					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20083		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/967
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/968
Concurrent Execution	06-Jul-2022	7	In GPU, there is a possible use after free	https://corp.mediatek.com/p	H-MED-MT68-200722/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**	roduct-security-bulletin/July-2022	
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/970
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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/July-2022	H-MED-MT68-200722/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/972
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/973
Concurrent Execution using Shared Resource with	06-Jul-2022	6.7	In TEEI driver, 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-bulletin/July-2022	H-MED-MT68-200722/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/975
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/977
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/978
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/980
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/981
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT68-200722/982

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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	bulletin/July-2022	
Incorrect Type Conversion or Cast	06-Jul-2022	6.7	In audio DSP, there is a possible memory corruption due to improper casting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558822; Issue ID: ALPS06558822. **CVE ID : CVE-2022-21786**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/983
Out-of-bounds Write	06-Jul-2022	6.7	In audio DSP, 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: ALPS06558844; Issue ID: ALPS06558844.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21787		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/985
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/986
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**		
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/988
Product: mt6889					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/990
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20082		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/992
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/993
Concurrent Execution using Shared Resource with Improper Synchroniz	06-Jul-2022	6.7	In GED driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			needed. User interaction is not needed for exploitation. Patch ID: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/995
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/997
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/998
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1000
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1001
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT68-200722/1002

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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	bulletin/July-2022	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1003
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21763		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1005
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1006
Product: mt6890					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT68-200722/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1008
Concurrent Execution using Shared Resource with Improper	06-Jul-2022	6.7	In TEEI driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1010
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21764		
Product: mt6891					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1012
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064;	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1014
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1015
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free due to improper locking. This could lead to local escalation of privilege	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1017
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21764		
Product: mt6893					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1019
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064;	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1021
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1022
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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-bulletin/July-2022	H-MED-MT68-200722/1023

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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1024
Improper Link Resolution Before File Access ('Link Following')	06-Jul-2022	6.7	In sound driver, there is a possible information disclosure due to symlink following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558663; Issue ID: ALPS06558663.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21770		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1026
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1027
Concurrent Execution using Shared Resource with Improper Synchroniz	06-Jul-2022	6.7	In TEEI driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			needed. User interaction is not needed for exploitation. Patch ID: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1029
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1031
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1032
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1034
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1035
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT68-200722/1036

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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	bulletin/July-2022	
Incorrect Type Conversion or Cast	06-Jul-2022	6.7	In audio DSP, there is a possible memory corruption due to improper casting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558822; Issue ID: ALPS06558822. **CVE ID : CVE-2022-21786**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1037
Out-of-bounds Write	06-Jul-2022	6.7	In audio DSP, 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: ALPS06558844; Issue ID: ALPS06558844.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21787		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1039
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1040
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**		
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1042
Product: mt6895					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1044
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21777		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1046
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1047
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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/July-2022	H-MED-MT68-200722/1048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**		
Improper Link Resolution Before File Access ('Link Following')	06-Jul-2022	6.7	In sound driver, there is a possible information disclosure due to symlink following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558663; Issue ID: ALPS06558663. **CVE ID : CVE-2022-21770**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1049
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1051
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1052
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1054
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1055
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT68-200722/1056

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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1057
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21783		
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1059
Incorrect Type Conversion or Cast	06-Jul-2022	6.7	In audio DSP, there is a possible memory corruption due to improper casting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558822; Issue ID: ALPS06558822. **CVE ID : CVE-2022-21786**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1060
Out-of-bounds Write	06-Jul-2022	6.7	In audio DSP, 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/July-2022	H-MED-MT68-200722/1061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06558844; Issue ID: ALPS06558844. **CVE ID : CVE-2022-21787**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1062
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1064
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT68-200722/1065
Product: mt6983					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1067
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1069
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1070
Improper Input Validation	06-Jul-2022	6.7	In CCCI, there is a possible out of bounds write due to a	https://corp.mediatek.com/product-	H-MED-MT69-200722/1071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	security-bulletin/July-2022	
Improper Link Resolution Before File Access ('Link Following')	06-Jul-2022	6.7	In sound driver, there is a possible information disclosure due to symlink following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558663; Issue ID: ALPS06558663. **CVE ID : CVE-2022-21770**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1072
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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/July-2022	H-MED-MT69-200722/1073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1074
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1075
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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-bulletin/July-2022	H-MED-MT69-200722/1076

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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1077
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1079
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1080
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1082
Incorrect Type Conversion or Cast	06-Jul-2022	6.7	In audio DSP, there is a possible memory corruption due to improper casting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558822; Issue ID: ALPS06558822. **CVE ID : CVE-2022-21786**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1083
Out-of-bounds Write	06-Jul-2022	6.7	In audio DSP, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT69-200722/1084

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: ALPS06558844; Issue ID: ALPS06558844. **CVE ID : CVE-2022-21787**	bulletin/July-2022	
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1085
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**		
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1087
Product: mt6985					
Affected Version(s): -					
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT69-200722/1089
Product: mt8163					
Affected Version(s): -					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1090
Product: mt8167					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT81-200722/1091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784430; Issue ID: ALPS06784430. **CVE ID : CVE-2022-21767**	bulletin/July-2022	
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1092
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21775		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1094
Product: mt8167s					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784351; Issue ID: ALPS06784351. **CVE ID : CVE-2022-21768**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1095
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of	https://corp.mediatek.com/product-security-	H-MED-MT81-200722/1096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	bulletin/July-2022	
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1097
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1099
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1100
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1102
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1103
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT81-200722/1104

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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	bulletin/July-2022	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1105
Product: mt8168					
Affected Version(s): -					
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1107
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1108
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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-bulletin/July-2022	H-MED-MT81-200722/1109

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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1110
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1112
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1113
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1115
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1116
Product: mt8173					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1117
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1118
Concurrent Execution using Shared Resource with Improper Synchronization	06-Jul-2022	6.4	In MDP, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			exploitation. Patch ID: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**		
Product: mt8175					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784430; Issue ID: ALPS06784430. **CVE ID : CVE-2022-21767**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1120
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784351; Issue ID: ALPS06784351. **CVE ID : CVE-2022-21768**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1122
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1123
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1125
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1126
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT81-200722/1127

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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	bulletin/July-2022	
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1128
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21785		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1130
Product: mt8183					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784430; Issue ID: ALPS06784430. **CVE ID : CVE-2022-21767**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1131
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, 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-MT81-200722/1132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784351; Issue ID: ALPS06784351. **CVE ID : CVE-2022-21768**	bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1133
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1135
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1136
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**		
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1138
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1139
Concurrent Execution using Shared Resource	06-Jul-2022	6.4	In MDP, 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-MT81-200722/1140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	bulletin/July-2022	
Product: mt8185					
Affected Version(s): -					
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1141
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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/July-2022	H-MED-MT81-200722/1142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**		
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1143
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1144
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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-bulletin/July-2022	H-MED-MT81-200722/1145

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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1146
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1148
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1149
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT81-200722/1151
Product: mt8321					
Affected Version(s): -					
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1153
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1154
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1156
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1157
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a	https://corp.mediatek.com/product-security-	H-MED-MT83-200722/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	bulletin/July-2022	
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1159
Product: mt8362a					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06784430; Issue ID: ALPS06784430. **CVE ID : CVE-2022-21767**		
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784351; Issue ID: ALPS06784351. **CVE ID : CVE-2022-21768**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1161
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1162
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free due to improper locking. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT83-200722/1163

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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1164
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21780		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1166
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1167
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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/July-2022	H-MED-MT83-200722/1168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**		
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1169
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1170
Concurrent Execution	06-Jul-2022	6.4	In MDP, there is a possible use after free	https://corp.mediatek.com/p	H-MED-MT83-200722/1171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	roduct-security-bulletin/July-2022	
Product: mt8365					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784430; Issue ID: ALPS06784430. **CVE ID : CVE-2022-21767**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1172
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS06784351; Issue ID: ALPS06784351. **CVE ID : CVE-2022-21768**		
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1174
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1175
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free due to improper locking. This could	https://corp.mediatek.com/product-security-	H-MED-MT83-200722/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1177
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21780		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1179
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1180
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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/July-2022	H-MED-MT83-200722/1181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**		
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1182
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1183
Concurrent Execution	06-Jul-2022	6.4	In MDP, there is a possible use after free	https://corp.mediatek.com/p	H-MED-MT83-200722/1184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	roduct-security-bulletin/July-2022	
Product: mt8385					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784430; Issue ID: ALPS06784430. **CVE ID : CVE-2022-21767**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1185
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS06784351; Issue ID: ALPS06784351. **CVE ID : CVE-2022-21768**		
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1187
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1188
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT83-200722/1189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1190
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21781		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1192
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1193
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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/July-2022	H-MED-MT83-200722/1194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1195
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT83-200722/1196
Product: mt8666					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1197
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1199
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1200
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**		
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1202
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1203
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission	https://corp.mediatek.com/product-security-	H-MED-MT86-200722/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	bulletin/July-2022	
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1205
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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/July-2022	H-MED-MT86-200722/1206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**		
Product: mt8667					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1207
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1209
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1210
Improper Input Validation	06-Jul-2022	6.7	In CCCI, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT86-200722/1211

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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1212
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21780		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1214
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1215
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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/July-2022	H-MED-MT86-200722/1216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**		
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1217
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1218
Concurrent Execution	06-Jul-2022	6.4	In MDP, there is a possible use after free	https://corp.mediatek.com/p	H-MED-MT86-200722/1219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	roduct-security-bulletin/July-2022	
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1220
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**		
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1222
Product: mt8675					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20083		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1224
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1226
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1227
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1229
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1230
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT86-200722/1231

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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1232
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21783		
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1234
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1235
Concurrent Execution using Shared Resource with Improper Synchroniz	06-Jul-2022	6.4	In MDP, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			needed. User interaction is not needed for exploitation. Patch ID: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1237
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1239
Product: mt8695					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1240
Product: mt8696					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT86-200722/1241

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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1242
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21781		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1244
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1245
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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/July-2022	H-MED-MT86-200722/1246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT86-200722/1247
Product: mt8735a					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883;	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1249
Product: mt8735b					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1251
Product: mt8765					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1253
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21777		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1255
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1256
Concurrent Execution using Shared Resource with Improper Synchroniz	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion due to a race condition. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			needed. User interaction is not needed for exploitation. Patch ID: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1258
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1260
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1261
Product: mt8766					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1263
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1265
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1266
Concurrent Execution using	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion due to a	https://corp.mediatek.com/product-	H-MED-MT87-200722/1267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**	security-bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1268
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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/July-2022	H-MED-MT87-200722/1269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1270
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1271
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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-bulletin/July-2022	H-MED-MT87-200722/1272

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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**		
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1273
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1275
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1276
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**		
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1278
Product: mt8768					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20083		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1280
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1282
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1283
Concurrent Execution using Shared Resource with Improper Synchronization	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			exploitation. Patch ID: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**		
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1285
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1286
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT87-200722/1287

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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1288
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21782		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1290
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1291
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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/July-2022	H-MED-MT87-200722/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1293
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1295
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1296
Product: mt8771					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1298
Product: mt8781					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1300
Product: mt8785					
Affected Version(s): -					
Concurrent Execution using Shared Resource	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion due to a race condition. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT87-200722/1301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**	bulletin/July-2022	
Product: mt8786					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1302
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1304
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21765		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1306
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1307
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1309
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1311
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1312
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**		
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1314
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1315
Concurrent Execution using Shared Resource	06-Jul-2022	6.4	In MDP, 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-MT87-200722/1316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	bulletin/July-2022	
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1317
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**		
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1319
Product: mt8788					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1321
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1322
Improper Input Validation	06-Jul-2022	6.7	In CCCI, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT87-200722/1323

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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	bulletin/July-2022	
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1324
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21772		
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1326
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1327
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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/July-2022	H-MED-MT87-200722/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1329
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1331
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1332
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1334
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1335
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a	https://corp.mediatek.com/product-security-	H-MED-MT87-200722/1336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	bulletin/July-2022	
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1337
Product: mt8789					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1339
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1341
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1342
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free due to improper locking. This could lead to local escalation of privilege	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1344
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1346
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1347
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**		
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1349
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1350
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission	https://corp.mediatek.com/product-security-	H-MED-MT87-200722/1351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	bulletin/July-2022	
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1352
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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/July-2022	H-MED-MT87-200722/1353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**		
Product: mt8791					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1354
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**		
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1356
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1357
Improper Input Validation	06-Jul-2022	6.7	In CCCI, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT87-200722/1358

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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	bulletin/July-2022	
Improper Link Resolution Before File Access ('Link Following')	06-Jul-2022	6.7	In sound driver, there is a possible information disclosure due to symlink following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558663; Issue ID: ALPS06558663. **CVE ID : CVE-2022-21770**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1359
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21772		
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1361
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1362
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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/July-2022	H-MED-MT87-200722/1363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1364
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1366
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1367
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**		
Incorrect Type Conversion or Cast	06-Jul-2022	6.7	In audio DSP, there is a possible memory corruption due to improper casting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558822; Issue ID: ALPS06558822. **CVE ID : CVE-2022-21786**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1369
Out-of-bounds Write	06-Jul-2022	6.7	In audio DSP, 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: ALPS06558844; Issue ID: ALPS06558844. **CVE ID : CVE-2022-21787**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1370
Concurrent Execution using Shared Resource	06-Jul-2022	6.4	In MDP, 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-MT87-200722/1371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	bulletin/July-2022	
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1372
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**		
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1374
Product: mt8797					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1376
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1377
Improper Input Validation	06-Jul-2022	6.7	In CCCI, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT87-200722/1378

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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	bulletin/July-2022	
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1379
Improper Link Resolution Before File Access ('Link Following')	06-Jul-2022	6.7	In sound driver, there is a possible information disclosure due to symlink following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558663; Issue ID: ALPS06558663.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21770		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842. **CVE ID : CVE-2022-21772**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1381
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free 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: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1382
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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/July-2022	H-MED-MT87-200722/1383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1384
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1386
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1387
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1389
Incorrect Type Conversion or Cast	06-Jul-2022	6.7	In audio DSP, there is a possible memory corruption due to improper casting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558822; Issue ID: ALPS06558822. **CVE ID : CVE-2022-21786**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1390
Out-of-bounds Write	06-Jul-2022	6.7	In audio DSP, there is a possible out of bounds write due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT87-200722/1391

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: ALPS06558844; Issue ID: ALPS06558844. **CVE ID : CVE-2022-21787**	bulletin/July-2022	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1392
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21763		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1394
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1395
Product: mt8798					
Affected Version(s): -					
Improper Link Resolution Before File Access	06-Jul-2022	6.7	In sound driver, there is a possible information disclosure due to symlink following.	https://corp.mediatek.com/product-security-	H-MED-MT87-200722/1396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Link Following')			This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558663; Issue ID: ALPS06558663. **CVE ID : CVE-2022-21770**	bulletin/July-2022	
Incorrect Type Conversion or Cast	06-Jul-2022	6.7	In audio DSP, there is a possible memory corruption due to improper casting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558822; Issue ID: ALPS06558822. **CVE ID : CVE-2022-21786**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1397
Out-of-bounds Write	06-Jul-2022	6.7	In audio DSP, 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: ALPS06558844; Issue ID: ALPS06558844.	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21787		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	H-MED-MT87-200722/1399
Vendor: Nvidia					
Product: dgx_a100					
Affected Version(s): -					
Out-of-bounds Write	02-Jul-2022	8.2	NVIDIA DGX A100 contains a vulnerability in SBIOS in the BiosCfgTool, where a local user with elevated privileges can read and write beyond intended bounds in SMRAM, which may lead to code execution, escalation of privileges, denial of service, and information disclosure. The scope of impact can extend to other components. **CVE ID : CVE-2022-28200**	https://nvidia.custhelp.com/app/answers/detail/a_id/5367	H-NVI-DGX_-200722/1400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	04-Jul-2022	8.2	NVIDIA DGX A100 contains a vulnerability in SBIOS in the Ofbd, where a local user with elevated privileges can cause access to an uninitialized pointer, which may lead to code execution, escalation of privileges, denial of service, and information disclosure. The scope of impact can extend to other components. **CVE ID : CVE-2022-31599**	https://nvidia.custhelp.com/app/answers/detail/a_id/5367	H-NVI-DGX_-200722/1401
Integer Overflow or Wraparound	04-Jul-2022	8.2	NVIDIA DGX A100 contains a vulnerability in SBIOS in the SmmCore, where a user with high privileges can chain another vulnerability to this vulnerability, causing an integer overflow, possibly leading to code execution, escalation of privileges, denial of service, compromised integrity, and information disclosure. The scope of impact can extend to other components. **CVE ID : CVE-2022-31600**	https://nvidia.custhelp.com/app/answers/detail/a_id/5367	H-NVI-DGX_-200722/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2022	6.7	NVIDIA DGX A100 contains a vulnerability in SBIOS in the SmbiosPei, which may allow a highly privileged local attacker to cause an out-of-bounds write, which may lead to code execution, denial of service, compromised integrity, and information disclosure. **CVE ID : CVE-2022-31601**	https://nvidia.custhelp.com/app/answers/detail/a_id/5367	H-NVI-DGX_-200722/1403
Out-of-bounds Write	04-Jul-2022	6.7	NVIDIA DGX A100 contains a vulnerability in SBIOS in the IpSecDxe, where a user with elevated privileges and a preconditioned heap can exploit an out-of-bounds write vulnerability, which may lead to code execution, denial of service, data integrity impact, and information disclosure. **CVE ID : CVE-2022-31602**	https://nvidia.custhelp.com/app/answers/detail/a_id/5367	H-NVI-DGX_-200722/1404
Improper Validation of Array Index	04-Jul-2022	6.7	NVIDIA DGX A100 contains a vulnerability in SBIOS in the IpSecDxe, where a user with high privileges and preconditioned IpSecDxe global data	https://nvidia.custhelp.com/app/answers/detail/a_id/5367	H-NVI-DGX_-200722/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can exploit improper validation of an array index to cause code execution, which may lead to denial of service, data integrity impact, and information disclosure. **CVE ID : CVE-2022-31603**		
Vendor: Omron					
Product: na5-12w					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NA5--200722/1406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NA5--200722/1407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34151		
Product: na5-15w					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NA5--200722/1408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NA5--200722/1409
Product: na5-7w					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-	H-OMR-NA5--200722/1410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NA5--200722/1411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Product: na5-9w					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NA5--200722/1412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NA5--200722/1413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Product: nj-pa3001					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ-P-200722/1414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ-P-200722/1415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ-P-200722/1416
Product: nj-pd3001					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ-P-200722/1417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ-P-200722/1418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ-P-200722/1419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nj101-1000					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ10-200722/1420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ10-200722/1421
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ10-200722/1422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj101-1020					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ10-200722/1423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ10-200722/1424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ10-200722/1425
Product: nj101-9000					
Affected Version(s): -					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	H-OMR-NJ10-200722/1426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ10-200722/1427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ10-200722/1428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj101-9020					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ10-200722/1429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ10-200722/1430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ10-200722/1431
Product: nj301-1100					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ30-200722/1432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ30-200722/1433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ30-200722/1434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nj301-1200					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ30-200722/1435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ30-200722/1436
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ30-200722/1437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj501-1300					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1440
Product: nj501-1320					
Affected Version(s): -					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	H-OMR-NJ50-200722/1441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj501-1340					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1446
Product: nj501-140					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nj501-1420					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1451
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj501-1500					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1455
Product: nj501-1520					
Affected Version(s): -					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	H-OMR-NJ50-200722/1456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj501-4300					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1461
Product: nj501-4310					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nj501-4320					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1466
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj501-4400					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1470
Product: nj501-4500					
Affected Version(s): -					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	H-OMR-NJ50-200722/1471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj501-5300					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1476
Product: nj501-r300					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nj501-r320					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1481
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj501-r400					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1485
Product: nj501-r420					
Affected Version(s): -					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	H-OMR-NJ50-200722/1486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj501-r500					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1491
Product: nj501-r520					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NJ50-200722/1493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NJ50-200722/1494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nx102-1000					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX10-200722/1495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX10-200722/1496
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX10-200722/1497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx102-1020					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX10-200722/1498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX10-200722/1499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX10-200722/1500
Product: nx102-1100					
Affected Version(s): -					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	H-OMR-NX10-200722/1501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX10-200722/1502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX10-200722/1503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx102-1120					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX10-200722/1504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX10-200722/1505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX10-200722/1506
Product: nx102-1200					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX10-200722/1507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX10-200722/1508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX10-200722/1509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nx102-1220					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX10-200722/1510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX10-200722/1511
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX10-200722/1512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx102-9020					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX10-200722/1513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX10-200722/1514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX10-200722/1515
Product: nx1p2-1040dt					
Affected Version(s): -					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	H-OMR-NX1P-200722/1516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1P-200722/1517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX1P-200722/1518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx1p2-1040dt1					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1P-200722/1519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1P-200722/1520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX1P-200722/1521
Product: nx1p2-1140dt					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1P-200722/1522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1P-200722/1523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX1P-200722/1524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nx1p2-1140dt1					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1P-200722/1525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1P-200722/1526
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX1P-200722/1527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx1p2-9024dt					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1P-200722/1528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1P-200722/1529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX1P-200722/1530
Product: nx1p2-9024dt1					
Affected Version(s): -					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	H-OMR-NX1P-200722/1531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1P-200722/1532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX1P-200722/1533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx1w-adb21					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1W-200722/1534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1W-200722/1535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX1W-200722/1536
Product: nx1w-cif01					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1W-200722/1537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1W-200722/1538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX1W-200722/1539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nx1w-cif11					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1W-200722/1540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1W-200722/1541
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX1W-200722/1542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx1w-cif12					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1W-200722/1543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1W-200722/1544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX1W-200722/1545
Product: nx1w-dab21v					
Affected Version(s): -					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	H-OMR-NX1W-200722/1546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1W-200722/1547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX1W-200722/1548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx1w-mab221					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1W-200722/1549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX1W-200722/1550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX1W-200722/1551
Product: nx701-1600					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX70-200722/1552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX70-200722/1553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX70-200722/1554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nx701-1620					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX70-200722/1555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX70-200722/1556
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX70-200722/1557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx701-1700					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX70-200722/1558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX70-200722/1559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX70-200722/1560
Product: nx701-1720					
Affected Version(s): -					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	H-OMR-NX70-200722/1561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX70-200722/1562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX70-200722/1563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx701-z600					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX70-200722/1564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX70-200722/1565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX70-200722/1566
Product: nx701-z700					
Affected Version(s): -					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX70-200722/1567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	H-OMR-NX70-200722/1568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	H-OMR-NX70-200722/1569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Vendor: Samsung					
Product: exynos_9820					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	12-Jul-2022	4.7	A possible race condition vulnerability in score driver prior to SMR Jul-2022 Release 1 can allow local attackers to interleave malicious operations. **CVE ID : CVE-2022-33691**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	H-SAM-EXYN-200722/1570
Vendor: Siemens					
Product: scalance_x200-4p_irt					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26649		
Product: scalance_x201-3p_irt					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x201-3p_irt_pro					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	H-SIE-SCAL-200722/1578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x202-2irt					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x202-2p_irt					
Affected Version(s): -					
Use of Insufficient	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	H-SIE-SCAL-200722/1583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6),	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x202-2p_irt_pro					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26649		
Product: scalance_x204-2					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x204-2fm					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	H-SIE-SCAL-200722/1593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x204-2ld					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x204-2ld_ts					
Affected Version(s): -					
Use of Insufficient	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	H-SIE-SCAL-200722/1598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6),	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x204-2ts					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26649		
Product: scalance_x204irt					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x204irt_pro					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	H-SIE-SCAL-200722/1608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x206-1					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x206-1ld					
Affected Version(s): -					
Use of Insufficient	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	H-SIE-SCAL-200722/1613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6),	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x208					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26649		
Product: scalance_x208_pro					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x212-2					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	H-SIE-SCAL-200722/1623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x212-2ld					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x216					
Affected Version(s): -					
Use of Insufficient	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	H-SIE-SCAL-200722/1628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6),	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x224					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26649		
Product: scalance_xf201-3p_irt					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_xf202-2p_irt					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	H-SIE-SCAL-200722/1638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_xf204					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_xf204-2					
Affected Version(s): -					
Use of Insufficient	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	H-SIE-SCAL-200722/1643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6),	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_xf204-2ba_irt					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26649		
Product: scalance_xf204irt					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_xf206-1					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	H-SIE-SCAL-200722/1653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_xf208					
Affected Version(s): -					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	H-SIE-SCAL-200722/1657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: simatic_cp_1242-7_v2					
Affected Version(s): -					
Improper Neutralization of Special	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions),	https://cert-portal.siemens.com/productce	H-SIE-SIMA-200722/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary	rt/pdf/ssa-517377.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: simatic_cp_1243-1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: simatic_cp_1243-7_lte_eu					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: simatic_cp_1243-7_lte_us					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34819		
Product: simatic_cp_1243-8_irc					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: simatic_cp_1542sp-1_irc					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: simatic_cp_1543-1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: simatic_cp_1543sp-1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIMA-200722/1681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: simatic_mv540_h					
Affected Version(s): -					
Insufficient Session Expiration	12-Jul-2022	8	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). The web session management of affected devices does not invalidate session ids in certain logout scenarios. This could allow an authenticated remote attacker to hijack other users' sessions. **CVE ID : CVE-2022-33137**	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	H-SIE-SIMA-200722/1682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	12-Jul-2022	7.5	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). Affected devices do not perform authentication for several web API endpoints. This could allow an unauthenticated remote attacker to read and download data from the device. **CVE ID : CVE-2022-33138**	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	H-SIE-SIMA-200722/1683
Product: simatic_mv540_s					
Affected Version(s): -					
Insufficient Session Expiration	12-Jul-2022	8	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). The web session	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	H-SIE-SIMA-200722/1684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management of affected devices does not invalidate session ids in certain logout scenarios. This could allow an authenticated remote attacker to hijack other users' sessions. **CVE ID : CVE-2022-33137**		
Missing Authentication for Critical Function	12-Jul-2022	7.5	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). Affected devices do not perform authentication for several web API endpoints. This could allow an unauthenticated remote attacker to read and download data from the device. **CVE ID : CVE-2022-33138**	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	H-SIE-SIMA-200722/1685
Product: simatic_mv550_h					
Affected Version(s): -					
Insufficient Session Expiration	12-Jul-2022	8	A vulnerability has been identified in SIMATIC MV540 H	https://cert-portal.siemens.com/productce	H-SIE-SIMA-200722/1686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). The web session management of affected devices does not invalidate session ids in certain logout scenarios. This could allow an authenticated remote attacker to hijack other users' sessions. **CVE ID : CVE-2022-33137**	rt/pdf/ssa-348662.pdf	
Missing Authentication for Critical Function	12-Jul-2022	7.5	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). Affected devices do not perform authentication for several web API endpoints. This could allow an	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	H-SIE-SIMA-200722/1687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote attacker to read and download data from the device. **CVE ID : CVE-2022-33138**		
Product: simatic_mv550_s					
Affected Version(s): -					
Insufficient Session Expiration	12-Jul-2022	8	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). The web session management of affected devices does not invalidate session ids in certain logout scenarios. This could allow an authenticated remote attacker to hijack other users' sessions. **CVE ID : CVE-2022-33137**	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	H-SIE-SIMA-200722/1688
Missing Authentication for Critical Function	12-Jul-2022	7.5	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3),	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	H-SIE-SIMA-200722/1689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). Affected devices do not perform authentication for several web API endpoints. This could allow an unauthenticated remote attacker to read and download data from the device. **CVE ID : CVE-2022-33138**		
Product: simatic_mv560_u					
Affected Version(s): -					
Insufficient Session Expiration	12-Jul-2022	8	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). The web session management of affected devices does not invalidate session ids in certain logout scenarios. This could allow an authenticated remote	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	H-SIE-SIMA-200722/1690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to hijack other users' sessions. **CVE ID : CVE-2022-33137**		
Missing Authentication for Critical Function	12-Jul-2022	7.5	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). Affected devices do not perform authentication for several web API endpoints. This could allow an unauthenticated remote attacker to read and download data from the device. **CVE ID : CVE-2022-33138**	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	H-SIE-SIMA-200722/1691
Product: simatic_mv560_x					
Affected Version(s): -					
Insufficient Session Expiration	12-Jul-2022	8	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3),	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	H-SIE-SIMA-200722/1692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). The web session management of affected devices does not invalidate session ids in certain logout scenarios. This could allow an authenticated remote attacker to hijack other users' sessions. **CVE ID : CVE-2022-33137**		
Missing Authentication for Critical Function	12-Jul-2022	7.5	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). Affected devices do not perform authentication for several web API endpoints. This could allow an unauthenticated remote attacker to read and download data from the device. **CVE ID : CVE-2022-33138**	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	H-SIE-SIMA-200722/1693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: siplus_et_200sp_cp_1542sp-1_irc_tx_rail					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: siplus_et_200sp_cp_1543sp-1_isec					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions),	https://cert-portal.siemens.com/productce	H-SIE-SIPL-200722/1699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to	rt/pdf/ssa-517377.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: siplus_et_200sp_cp_1543sp-1_isec_tx_rail					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: siplus_net_cp_1242-7_v2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions),	https://cert-portal.siemens.com/productce	H-SIE-SIPL-200722/1704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**	rt/pdf/ssa-517377.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: siplus_net_cp_1543-1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: siplus_s7-1200_cp_1243-1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: siplus_s7-1200_cp_1243-1_rail					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0),	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	H-SIE-SIPL-200722/1714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Vendor: Tenda					
Product: ac10					
Affected Version(s): 1.0					
Improper Control of	07-Jul-2022	9.8	Tenda AC10 US_AC10V1.0RTL_V1	https://github.com/winmt/C	H-TEN-AC10-200722/1715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			5.03.06.26_multi_TD01 was discovered to contain a remote code execution (RCE) vulnerability via the lanIp parameter. **CVE ID : CVE-2022-32054**	VE/blob/main/Tenda%20AC10/README.md	
Product: ax1803					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	9.8	Tenda AX1803 v1.0.0.1_2890 was discovered to contain a command injection vulnerability via the function setipv6status. **CVE ID : CVE-2022-34595**	N/A	H-TEN-AX18-200722/1716
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	9.8	Tenda AX1803 v1.0.0.1_2890 was discovered to contain a command injection vulnerability via the function WanParameterSetting. **CVE ID : CVE-2022-34596**	N/A	H-TEN-AX18-200722/1717
Product: ax1806					
Affected Version(s): -					
Out-of-bounds Write	01-Jul-2022	9.8	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the deviceList parameter in the function formAddMacfilterRule.	N/A	H-TEN-AX18-200722/1718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32032		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	9.8	Tenda AX1806 v1.0.0.1 was discovered to contain a command injection vulnerability via the function WanParameterSetting. **CVE ID : CVE-2022-34597**	N/A	H-TEN-AX18-200722/1719
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the list parameter in the function formSetQosBand. **CVE ID : CVE-2022-32030**	N/A	H-TEN-AX18-200722/1720
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the list parameter in the function fromSetRouteStatic. **CVE ID : CVE-2022-32031**	N/A	H-TEN-AX18-200722/1721
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the function formSetVirtualSer. **CVE ID : CVE-2022-32033**	N/A	H-TEN-AX18-200722/1722
Product: m3					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the function formSetAPCfg. **CVE ID : CVE-2022-32037**	N/A	H-TEN-M3-200722/1723
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the listN parameter in the function fromDhcpListClient. **CVE ID : CVE-2022-32039**	N/A	H-TEN-M3-200722/1724
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the function formSetCfm. **CVE ID : CVE-2022-32040**	N/A	H-TEN-M3-200722/1725
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the function formGetPassengerAnalyseData. **CVE ID : CVE-2022-32041**	N/A	H-TEN-M3-200722/1726
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the function formSetAccessCodeInfo.	N/A	H-TEN-M3-200722/1727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32043		
Vendor: Tendacn					
Product: ac23_ac2100					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	Tenda AC23 v16.03.07.44 was discovered to contain a stack overflow via the AdvSetMacMtuWan function. **CVE ID : CVE-2022-32383**	N/A	H-TEN-AC23-200722/1728
Out-of-bounds Write	06-Jul-2022	9.8	Tenda AC23 v16.03.07.44 is vulnerable to Stack Overflow that will allow for the execution of arbitrary code (remote). **CVE ID : CVE-2022-32385**	N/A	H-TEN-AC23-200722/1729
Out-of-bounds Write	06-Jul-2022	9.8	Tenda AC23 v16.03.07.44 was discovered to contain a buffer overflow via fromAdvSetMacMtuWan. **CVE ID : CVE-2022-32386**	N/A	H-TEN-AC23-200722/1730
Out-of-bounds Write	01-Jul-2022	8.8	Tenda AC23 v16.03.07.44 was discovered to contain a stack overflow via the security_5g parameter in the function formWifiBasicSet.	N/A	H-TEN-AC23-200722/1731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32384		
Product: m3					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the items parameter in the function formdelMasteraclist. **CVE ID : CVE-2022-32034**	N/A	H-TEN-M3-200722/1732
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the function formMasterMng. **CVE ID : CVE-2022-32035**	N/A	H-TEN-M3-200722/1733
Out-of-bounds Write	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to contain multiple stack overflow vulnerabilities via the ssidList, storeName, and trademark parameters in the function formSetStoreWeb. **CVE ID : CVE-2022-32036**	N/A	H-TEN-M3-200722/1734
Vendor: totolink					
Product: a3000ru					
Affected Version(s): -					
Improper Neutralization of Special	06-Jul-2022	7.2	Totolink A830R V5.9c.4729_B20191112, Totolink A3100R V4.1.2cu.5050_B2020	N/A	H-TOT-A300-200722/1735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			0504, Totolink A950RG V4.1.2cu.5161_B20200903, Totolink A800R V4.1.2cu.5137_B20200730, Totolink A3000RU V5.9c.5185_B20201128, Totolink A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability. **CVE ID : CVE-2022-28935**		
Product: a3100r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	7.2	Totolink A830R V5.9c.4729_B20191112, Totolink A3100R V4.1.2cu.5050_B20200504, Totolink A950RG V4.1.2cu.5161_B20200903, Totolink A800R V4.1.2cu.5137_B20200730, Totolink A3000RU V5.9c.5185_B20201128, Totolink A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability. **CVE ID : CVE-2022-28935**	N/A	H-TOT-A310-200722/1736
Product: a800r					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	7.2	Totolink A830R V5.9c.4729_B20191112, Totolink A3100R V4.1.2cu.5050_B20200504, Totolink A950RG V4.1.2cu.5161_B20200903, Totolink A800R V4.1.2cu.5137_B20200730, Totolink A3000RU V5.9c.5185_B20201128, Totolink A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability. **CVE ID : CVE-2022-28935**	N/A	H-TOT-A800-200722/1737
Product: a810r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	7.2	Totolink A830R V5.9c.4729_B20191112, Totolink A3100R V4.1.2cu.5050_B20200504, Totolink A950RG V4.1.2cu.5161_B20200903, Totolink A800R V4.1.2cu.5137_B20200730, Totolink A3000RU V5.9c.5185_B20201128, Totolink A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability. **CVE ID : CVE-2022-28935**	N/A	H-TOT-A810-200722/1738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: a830r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	7.2	Totolink A830R V5.9c.4729_B20191112, Totolink A3100R V4.1.2cu.5050_B20200504, Totolink A950RG V4.1.2cu.5161_B20200903, Totolink A800R V4.1.2cu.5137_B20200730, Totolink A3000RU V5.9c.5185_B20201128, Totolink A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability. **CVE ID : CVE-2022-28935**	N/A	H-TOT-A830-200722/1739
Product: a950rg					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	7.2	Totolink A830R V5.9c.4729_B20191112, Totolink A3100R V4.1.2cu.5050_B20200504, Totolink A950RG V4.1.2cu.5161_B20200903, Totolink A800R V4.1.2cu.5137_B20200730, Totolink A3000RU V5.9c.5185_B20201128, Totolink A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability.	N/A	H-TOT-A950-200722/1740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28935		
Product: ex300_v2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jul-2022	9.8	TOTOLINK EX300_V2 V4.0.3c.7484 was discovered to contain a command injection vulnerability via the langType parameter in the setLanguageCfg function. This vulnerability is exploitable via a crafted MQTT data packet. **CVE ID : CVE-2022-32449**	N/A	H-TOT-EX30-200722/1741
Product: t6					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the password parameter in the function FUN_00413f80. **CVE ID : CVE-2022-32044**	https://github.com/d1tto/IoT-vuln/tree/main/Totolink/T6-v2/5.setWiFiRepeaterCfg	H-TOT-T6-200722/1742
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the desc parameter in the function FUN_00413be4. **CVE ID : CVE-2022-32045**	N/A	H-TOT-T6-200722/1743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the desc parameter in the function FUN_0041880c. **CVE ID : CVE-2022-32046**	N/A	H-TOT-T6-200722/1744
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the desc parameter in the function FUN_00412ef4. **CVE ID : CVE-2022-32047**	N/A	H-TOT-T6-200722/1745
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the command parameter in the function FUN_0041cc88. **CVE ID : CVE-2022-32048**	N/A	H-TOT-T6-200722/1746
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the url parameter in the function FUN_00418540. **CVE ID : CVE-2022-32049**	N/A	H-TOT-T6-200722/1747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the cloneMac parameter in the function FUN_0041af40. **CVE ID : CVE-2022-32050**	N/A	H-TOT-T6-200722/1748
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the desc, week, sTime, eTime parameters in the function FUN_004133c4. **CVE ID : CVE-2022-32051**	N/A	H-TOT-T6-200722/1749
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the desc parameter in the function FUN_004137a4. **CVE ID : CVE-2022-32052**	N/A	H-TOT-T6-200722/1750
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the cloneMac parameter in the function FUN_0041621c. **CVE ID : CVE-2022-32053**	N/A	H-TOT-T6-200722/1751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wavlink					
Product: wl-wn575a3					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jul-2022	9.8	Wavlink WL-WN575A3 RPT75A3.V4300.201217 was discovered to contain a command injection vulnerability via the function obtw. This vulnerability allows attackers to execute arbitrary commands via a crafted POST request. **CVE ID : CVE-2022-34592**	N/A	H-WAV-WL-W-200722/1752
Vendor: webhmi					
Product: webhmi					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2022	9.1	A user with administrative privileges in Distributed Data Systems WebHMI 4.1.1.7662 may send OS commands to execute on the host server. **CVE ID : CVE-2022-2253**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-181-04	H-WEB-WEBH-200722/1753
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jul-2022	4.8	A user with administrative privileges in Distributed Data Systems WebHMI 4.1.1.7662 can store a script that could impact other logged in users.	https://www.cisa.gov/uscert/ics/advisories/icsa-22-181-04	H-WEB-WEBH-200722/1754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2254		
Vendor: Yokogawa					
Product: aw810d					
Affected Version(s): -					
Use of Insufficiently Random Values	04-Jul-2022	7.5	Use of insufficiently random values vulnerability exists in Vnet/IP communication module VI461 of YOKOGAWA Wide Area Communication Router (WAC Router) AW810D, which may allow a remote attacker to cause denial-of-service (DoS) condition by sending a specially crafted packet. **CVE ID : CVE-2022-32284**	https://web-material3.yokogawa.com/19/32825/files/YSAR-22-0005-J.pdf, https://web-material3.yokogawa.com/1/32825/files/YSAR-22-0005-E.pdf	H-YOK-AW81-200722/1755
Operating System					
Vendor: amperecomputing					
Product: ampere_altra_firmware					
Affected Version(s): * Up to (excluding) 1.09					
Incorrect Authorization	01-Jul-2022	9.8	On Ampere Altra and AltraMax devices before SRP 1.09, the the Altra reference design of UEFI accesses allows insecure access to SPI-NOR by the OS/hypervisor component. **CVE ID : CVE-2022-32295**	https://amperecomputing.com	O-AMP-AMPE-210722/1756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ampere_altra_max_firmware					
Affected Version(s): * Up to (excluding) 1.09					
Incorrect Authorization	01-Jul-2022	9.8	On Ampere Altra and AltraMax devices before SRP 1.09, the the Altra reference design of UEFI accesses allows insecure access to SPI-NOR by the OS/hypervisor component. **CVE ID : CVE-2022-32295**	https://amperecomputing.com	O-AMP-AMPE-210722/1757
Vendor: Apple					
Product: macos					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	01-Jul-2022	7	The Automox Agent installation package before 37 on macOS allows an unprivileged user to obtain root access because of incorrect access control on a file used within the PostInstall script. **CVE ID : CVE-2022-27904**	https://automox.com, https://www.automox.com/security/security-bulletin	O-APP-MACO-210722/1758
Vendor: Asus					
Product: dsl-n14u-b1_firmware					
Affected Version(s): 1.1.2.3_805					
Improper Neutralization of Input During Web Page Generation	01-Jul-2022	5.4	Cross Site Scripting (XSS) vulnerability in router Asus DSL-N14U-B1 1.1.2.3_805 via the "*list" parameters (e.g. filter_lwlist, keyword_rulelist, etc)	N/A	O-ASU-DSL--210722/1759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			in every ".asp" page containing a list of stored strings. The following asp files are affected: (1) cgi-bin/APP_Installation.asp, (2) cgi-bin/Advanced_ACL_Content.asp, (3) cgi-bin/Advanced_ADSL_Content.asp, (4) cgi-bin/Advanced_ASUSDDNS_Content.asp, (5) cgi-bin/Advanced_AiDisk_ftp.asp, (6) cgi-bin/Advanced_AiDisk_samba.asp, (7) cgi-bin/Advanced_DSL_Content.asp, (8) cgi-bin/Advanced_Firewall_Content.asp, (9) cgi-bin/Advanced_FirmwareUpgrade_Content.asp, (10) cgi-bin/Advanced_GWStaticRoute_Content.asp, (11) cgi-bin/Advanced_IPTV_Content.asp, (12) cgi-bin/Advanced_IPv6_Content.asp, (13) cgi-bin/Advanced_KeywordFilter_Content.asp, (14) cgi-bin/Advanced_LAN_Content.asp, (15) cgi-bin/Advanced_Modem_Content.asp, (16) cgi-bin/Advanced_PortTrigger_Content.asp, (17) cgi-bin/Advanced_QOSUs		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			erPrio_Content.asp, (18) cgi-bin/Advanced_QOSUserRules_Content.asp, (19) cgi-bin/Advanced_SettingBackup_Content.asp, (20) cgi-bin/Advanced_System_Content.asp, (21) cgi-bin/Advanced_URLFilter_Content.asp, (22) cgi-bin/Advanced_VPN_PPTP.asp, (23) cgi-bin/Advanced_VirtualServer_Content.asp, (24) cgi-bin/Advanced_WANPort_Content.asp, (25) cgi-bin/Advanced_WAdvanced_Content.asp, (26) cgi-bin/Advanced_WMode_Content.asp, (27) cgi-bin/Advanced_WWPS_Content.asp, (28) cgi-bin/Advanced_Wireless_Content.asp, (29) cgi-bin/Bandwidth_Limiter.asp, (30) cgi-bin/Guest_network.asp, (31) cgi-bin/Main_AccessLog_Content.asp, (32) cgi-bin/Main_AdslStatus_Content.asp, (33) cgi-bin/Main_Spectrum_Content.asp, (34) cgi-bin/Main_WebHistor		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			y_Content.asp, (35) cgi-bin/ParentalControl.asp, (36) cgi-bin/QIS_wizard.asp, (37) cgi-bin/QoS_EZQoS.asp, (38) cgi-bin/aidisk.asp, (39) cgi-bin/aidisk/Aidisk-1.asp, (40) cgi-bin/aidisk/Aidisk-2.asp, (41) cgi-bin/aidisk/Aidisk-3.asp, (42) cgi-bin/aidisk/Aidisk-4.asp, (43) cgi-bin/blocking.asp, (44) cgi-bin/cloud_main.asp, (45) cgi-bin/cloud_router_sync.asp, (46) cgi-bin/cloud_settings.asp, (47) cgi-bin/cloud_sync.asp, (48) cgi-bin/device-map/DSL_dashboard.asp, (49) cgi-bin/device-map/clients.asp, (50) cgi-bin/device-map/disk.asp, (51) cgi-bin/device-map/internet.asp, (52) cgi-bin/error_page.asp, (53) cgi-bin/index.asp, (54) cgi-bin/index2.asp, (55) cgi-bin/qis/QIS_PTM_manual_setting.asp, (56) cgi-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/qis/QIS_admin_pass.asp, (57) cgi-bin/qis/QIS_annex_setting.asp, (58) cgi-bin/qis/QIS_bridge_cfg_tmp.asp, (59) cgi-bin/qis/QIS_detect.asp, (60) cgi-bin/qis/QIS_finish.asp, (61) cgi-bin/qis/QIS_ipoa_cfg_tmp.asp, (62) cgi-bin/qis/QIS_manual_setting.asp, (63) cgi-bin/qis/QIS_mer_cfg.asp, (64) cgi-bin/qis/QIS_mer_cfg_tmp.asp, (65) cgi-bin/qis/QIS_ppp_cfg.asp, (66) cgi-bin/qis/QIS_ppp_cfg_tmp.asp, (67) cgi-bin/qis/QIS_wireless.asp, (68) cgi-bin/query_wan_status.asp, (69) cgi-bin/query_wan_status2.asp, and (70) cgi-bin/start_apply.asp. **CVE ID : CVE-2022-32988**		
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
Improper Neutralization of Special Elements in Output Used by a Downstrea	01-Jul-2022	6.5	GnuPG through 2.3.6, in unusual situations where an attacker possesses any secret-key information from a victim's keyring and other constraints (e.g., use of GPGME)	https://dev.gnupg.org/T6027, https://bugs.debian.org/1014157	O-DEB-DEBI-210722/1760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')			are met, allows signature forgery via injection into the status line. **CVE ID : CVE-2022-34903**		
Affected Version(s): 11.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-Jul-2022	6.5	GnuPG through 2.3.6, in unusual situations where an attacker possesses any secret-key information from a victim's keyring and other constraints (e.g., use of GPGME) are met, allows signature forgery via injection into the status line. **CVE ID : CVE-2022-34903**	https://dev.gnupg.org/T6027, https://bugs.debian.org/1014157	O-DEB-DEBI-210722/1761
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 36					
Inadequate Encryption Strength	05-Jul-2022	7.5	AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext	https://www.openssl.org/news/secadv/20220705.txt, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=a98f339ddd7e8f487d6e0088d4a9a42324885a93, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=919925673	O-FED-FEDO-210722/1762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p). **CVE ID : CVE-2022-2097**	d6c9cfed3c1085497f5dfbbed5fc431	
Exposure of Sensitive Information to an Unauthorized Actor	05-Jul-2022	7.1	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-	https://xenbits.xenproject.org/xsa/advisory-403.txt, http://xenbits.xen.org/xsa/advisory-403.html, http://www.openwall.com/lists/oss-security/2022/07/05/6	O-FED-FEDO-210722/1763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			33741, CVE-2022-33742). **CVE ID : CVE-2022-26365**		
Exposure of Sensitive Information to an Unauthorized Actor	05-Jul-2022	7.1	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742). **CVE ID : CVE-2022-33740**	https://xenbits.xenproject.org/xsa/advisory-403.txt, http://xenbits.xen.org/xsa/advisory-403.html, http://www.openwall.com/lists/oss-security/2022/07/05/6	O-FED-FEDO-210722/1764
Exposure of Sensitive Information to an	05-Jul-2022	7.1	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text	https://xenbits.xenproject.org/xsa/advisory-403.txt, http://xenbits.xen.org/xsa/ad	O-FED-FEDO-210722/1765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742). **CVE ID : CVE-2022-33741**	visory-403.html, http://www.openwall.com/lists/oss-security/2022/07/05/6	
Exposure of Sensitive Information to an Unauthorized Actor	05-Jul-2022	7.1	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365,	https://xenbits.xenproject.org/xsa/advisory-403.txt, http://xenbits.xen.org/xsa/advisory-403.html, http://www.openwall.com/lists/oss-security/2022/07/05/6	O-FED-FEDO-210722/1766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742). **CVE ID : CVE-2022-33742**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-Jul-2022	6.5	GnuPG through 2.3.6, in unusual situations where an attacker possesses any secret-key information from a victim's keyring and other constraints (e.g., use of GPGME) are met, allows signature forgery via injection into the status line. **CVE ID : CVE-2022-34903**	https://dev.gnupg.org/T6027, https://bugs.debian.org/1014157	O-FED-FEDO-210722/1767
Vendor: gallagher					
Product: controller_6000_firmware					
Affected Version(s): From (including) 8.30 Up to (excluding) 8.30.220303a					
N/A	06-Jul-2022	7.5	Gallagher Controller 6000 is vulnerable to a Denial of Service attack via conflicting ARP packets with a duplicate IP address. This issue affects: Gallagher Gallagher	https://security.gallagher.com/Security-Advisories/CVE-2022-26078	O-GAL-CONT-210722/1768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller 6000 vCR8.60 versions prior to 220303a; vCR8.50 versions prior to 220303a; vCR8.40 versions prior to 220303a; vCR8.30 versions prior to 220303a. **CVE ID : CVE-2022-26078**		
Affected Version(s): From (including) 8.40 Up to (excluding) 8.40.220303a					
N/A	06-Jul-2022	7.5	Gallagher Controller 6000 is vulnerable to a Denial of Service attack via conflicting ARP packets with a duplicate IP address. This issue affects: Gallagher Gallagher Controller 6000 vCR8.60 versions prior to 220303a; vCR8.50 versions prior to 220303a; vCR8.40 versions prior to 220303a; vCR8.30 versions prior to 220303a. **CVE ID : CVE-2022-26078**	https://security.gallagher.com/Security-Advisories/CVE-2022-26078	O-GAL-CONT-210722/1769
Affected Version(s): From (including) 8.50 Up to (excluding) 8.50.220303a					
N/A	06-Jul-2022	7.5	Gallagher Controller 6000 is vulnerable to a Denial of Service attack via conflicting ARP packets with a duplicate IP address. This issue affects: Gallagher Gallagher Controller 6000 vCR8.60 versions	https://security.gallagher.com/Security-Advisories/CVE-2022-26078	O-GAL-CONT-210722/1770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 220303a; vCR8.50 versions prior to 220303a; vCR8.40 versions prior to 220303a; vCR8.30 versions prior to 220303a. **CVE ID : CVE-2022-26078**		
Affected Version(s): From (including) 8.60 Up to (excluding) 8.60.220303a					
N/A	06-Jul-2022	7.5	Gallagher Controller 6000 is vulnerable to a Denial of Service attack via conflicting ARP packets with a duplicate IP address. This issue affects: Gallagher Gallagher Controller 6000 vCR8.60 versions prior to 220303a; vCR8.50 versions prior to 220303a; vCR8.40 versions prior to 220303a; vCR8.30 versions prior to 220303a. **CVE ID : CVE-2022-26078**	https://security.gallagher.com/Security-Advisories/CVE-2022-26078	O-GAL-CONT-210722/1771
Vendor: Google					
Product: android					
Affected Version(s): 10.0					
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS06784430; Issue ID: ALPS06784430. **CVE ID : CVE-2022-21767**		
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784351; Issue ID: ALPS06784351. **CVE ID : CVE-2022-21768**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1773
Improper Input Validation	12-Jul-2022	7.8	Improper validation vulnerability in ucmRetParcelable of KnoxSDK prior to SMR Jul-2022 Release 1 allows attackers to launch certain activities. **CVE ID : CVE-2022-33704**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1774
Improper Authentication	12-Jul-2022	7.8	Improper authentication vulnerability in AppLock prior to SMR Jul-2022 Release 1 allows attacker to bypass password confirm activity by	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hijacking the implicit intent. **CVE ID : CVE-2022-30755**		
N/A	12-Jul-2022	7.8	Implicit Intent hijacking vulnerability in Finder prior to SMR Jul-2022 Release 1 allow allows attackers to launch certain activities with privilege of Finder. **CVE ID : CVE-2022-30756**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1776
Improper Input Validation	12-Jul-2022	7.8	Improper validation vulnerability in CACertificateInfo prior to SMR Jul-2022 Release 1 allows attackers to launch certain activities. **CVE ID : CVE-2022-33703**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1777
Incorrect Permission Assignment for Critical Resource	12-Jul-2022	7.8	Use of improper permission in InputManagerService prior to SMR Jul-2022 Release 1 allows unauthorized access to the service. **CVE ID : CVE-2022-33695**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1778
N/A	12-Jul-2022	7.8	Implicit Intent hijacking vulnerability in AppLinker prior to SMR Jul-2022 Release 1 allow allows attackers to launch certain activities with	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege of AppLinker. **CVE ID : CVE-2022-30754**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1780
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1781
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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-bulletin/July-2022	O-GOO-ANDR-210722/1782

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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**		
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1783
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717.	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21764		
Incorrect Default Permissions	12-Jul-2022	5.5	Implicit Intent hijacking vulnerability in Finder prior to SMR Jul-2022 Release 1 allow allows attackers to access some protected information with privilege of Finder. **CVE ID : CVE-2022-30758**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1785
Incorrect Authorization	12-Jul-2022	5.5	Improper authorization vulnerability in Knoxguard prior to SMR Jul-2022 Release 1 allows local attacker to disable keyguard and bypass Knoxguard lock by factory reset. **CVE ID : CVE-2022-33702**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1786
N/A	12-Jul-2022	5.5	Unprotected dynamic receiver in Wearable Manager Service prior to SMR Jul-2022 Release 1 allows attacker to launch arbitray activity and access senstive information. **CVE ID : CVE-2022-33685**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1787
Time-of-check Time-of-use (TOCTOU)	12-Jul-2022	4.7	A possible race condition vulnerability in score driver prior to SMR Jul-2022 Release 1	https://security.samsungmobile.com/securityUpdate.smsb?	O-GOO-ANDR-210722/1788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			can allow local attackers to interleave malicious operations. **CVE ID : CVE-2022-33691**	year=2022&month=7	
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1789
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Improper access control vulnerability in updateLastConnectedClientInfo function of SemWifiApClient prior to SMR Jul-2022 Release 1 allows attacker to access wifi ap client mac address that connected. **CVE ID : CVE-2022-30750**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1790
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Improper access control vulnerability in sendDHCPACKBroadcast function of SemWifiApClient prior to SMR Jul-2022	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Release 1 allows attacker to access wifi ap client mac address that connected by using WIFI_AP_STA_DHCPACK_EVENT action. **CVE ID : CVE-2022-30751**		
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Improper access control vulnerability in sendDHCPACKBroadcast function of SemWifiApClient prior to SMR Jul-2022 Release 1 allows attacker to access wifi ap client mac address that connected by using WIFI_AP_STA_STATE_CHANGED action. **CVE ID : CVE-2022-30752**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1792
Incorrect Default Permissions	12-Jul-2022	3.3	Improper use of a unique device ID in unprotected SecSoterService prior to SMR Jul-2022 Release 1 allows local attackers to get the device ID without permission. **CVE ID : CVE-2022-30753**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1793
Insertion of Sensitive Information into Log File	12-Jul-2022	3.3	Exposure of Sensitive Information in telephony-common.jar prior to SMR Jul-2022 Release 1 allows local	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to access IMSI via log. **CVE ID : CVE-2022-33687**		
Insertion of Sensitive Information into Log File	12-Jul-2022	3.3	Sensitive information exposure vulnerability in EventType in SecTelephonyProvider prior to SMR Jul-2022 Release 1 allows local attackers with log access permission to get IMSI through device log. **CVE ID : CVE-2022-33688**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1795
Incorrect Permission Assignment for Critical Resource	12-Jul-2022	3.3	Improper access control vulnerability in TelephonyUI prior to SMR Jul-2022 Release 1 allows attackers to change preferred network type by unprotected binder call. **CVE ID : CVE-2022-33689**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1796
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Exposure of Sensitive Information in CSC application prior to SMR Jul-2022 Release 1 allows local attacker to access wifi information via unprotected intent broadcasting. **CVE ID : CVE-2022-33694**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1797
Insertion of Sensitive	12-Jul-2022	3.3	Sensitive information exposure	https://security.samsungmob	O-GOO-ANDR-210722/1798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information into Log File			vulnerability in ImsServiceSwitchBase in ImsCore prior to SMR Jul-2022 Release 1 allows local attackers with log access permission to get IMSI through device log. **CVE ID : CVE-2022-33697**	ile.com/securityUpdate.smsb?year=2022&month=7	
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Exposure of Sensitive Information in Telecom application prior to SMR Jul-2022 Release 1 allows local attackers to access ICCID via log. **CVE ID : CVE-2022-33698**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1799
Inclusion of Functionality from Untrusted Control Sphere	12-Jul-2022	3.3	Improper access control vulnerability in KnoxCustomManagerService prior to SMR Jul-2022 Release 1 allows attacker to call PowerManaer.goToSleep method which is protected by system permission by sending braodcast intent. **CVE ID : CVE-2022-33701**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1800
Incorrect Authorization	12-Jul-2022	3.3	Improper authorization in isemtelephony prior to SMR Jul-2022 Release 1 allows attacker to obtain CID without	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACCESS_FINE_LOCATION permission. **CVE ID : CVE-2022-30757**		
Files or Directories Accessible to External Parties	12-Jul-2022	2.3	Exposure of Sensitive Information in GsmAlarmManager prior to SMR Jul-2022 Release 1 allows local attacker to access iccid via log. **CVE ID : CVE-2022-33686**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1802
Insertion of Sensitive Information into Log File	12-Jul-2022	2.3	Exposure of Sensitive Information in CID Manager prior to SMR Jul-2022 Release 1 allows local attacker to access iccid via log. **CVE ID : CVE-2022-33693**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1803
Exposure of Resource to Wrong Sphere	12-Jul-2022	2.3	Exposure of Sensitive Information in getDsaSimImsi in TelephonyUI prior to SMR Jul-2022 Release 1 allows local attacker to access imsi via log. **CVE ID : CVE-2022-33699**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1804
Exposure of Resource to Wrong Sphere	12-Jul-2022	2.3	Exposure of Sensitive Information in putDsaSimImsi in TelephonyUI prior to SMR Jul-2022 Release 1 allows local attacker to access imsi via log. **CVE ID : CVE-2022-33700**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 11.0					
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784351; Issue ID: ALPS06784351. **CVE ID : CVE-2022-21768**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1806
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784430; Issue ID: ALPS06784430. **CVE ID : CVE-2022-21767**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1807
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894. **CVE ID : CVE-2022-21777**		
Improper Input Validation	12-Jul-2022	7.8	Improper validation vulnerability in CACertificateInfo prior to SMR Jul-2022 Release 1 allows attackers to launch certain activities. **CVE ID : CVE-2022-33703**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1809
N/A	12-Jul-2022	7.8	Implicit Intent hijacking vulnerability in AppLinker prior to SMR Jul-2022 Release 1 allow allows attackers to launch certain activities with privilege of AppLinker. **CVE ID : CVE-2022-30754**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1810
N/A	12-Jul-2022	7.8	Implicit Intent hijacking vulnerability in Finder prior to SMR Jul-2022 Release 1 allow allows attackers to launch certain activities with privilege of Finder. **CVE ID : CVE-2022-30756**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Jul-2022	7.8	Improper validation vulnerability in ucmRetParcelable of KnoxSDK prior to SMR Jul-2022 Release 1 allows attackers to launch certain activities. **CVE ID : CVE-2022-33704**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1812
Improper Authentication	12-Jul-2022	7.8	Improper authentication vulnerability in AppLock prior to SMR Jul-2022 Release 1 allows attacker to bypass password confirm activity by hijacking the implicit intent. **CVE ID : CVE-2022-30755**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1813
Incorrect Permission Assignment for Critical Resource	12-Jul-2022	7.8	Use of improper permission in InputManagerService prior to SMR Jul-2022 Release 1 allows unauthorized access to the service. **CVE ID : CVE-2022-33695**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1814
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1816
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1817
Improper Link Resolution Before File Access	06-Jul-2022	6.7	In sound driver, there is a possible information disclosure due to symlink following.	https://corp.mediatek.com/product-security-	O-GOO-ANDR-210722/1818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Link Following')			This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558663; Issue ID: ALPS06558663. **CVE ID : CVE-2022-21770**	bulletin/July-2022	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1819
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842.	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21772		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1821
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1822
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**		
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1824
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1825
Incorrect Type	06-Jul-2022	6.7	In audio DSP, there is a possible memory	https://corp.mediatek.com/p	O-GOO-ANDR-210722/1826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			corruption due to improper casting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558822; Issue ID: ALPS06558822. **CVE ID : CVE-2022-21786**	roduct-security-bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	6.7	In audio DSP, 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: ALPS06558844; Issue ID: ALPS06558844. **CVE ID : CVE-2022-21787**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1827
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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/July-2022	O-GOO-ANDR-210722/1828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1829
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1830
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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-bulletin/July-2022	O-GOO-ANDR-210722/1831

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: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1832
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450. **CVE ID : CVE-2022-21776**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1834
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1835
Incorrect Default Permissions	12-Jul-2022	5.5	Implicit Intent hijacking vulnerability in Finder prior to SMR Jul-2022 Release 1 allow allows attackers to access some protected information	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with privilege of Finder. **CVE ID : CVE-2022-30758**		
N/A	12-Jul-2022	5.5	Unprotected dynamic receiver in Wearable Manager Service prior to SMR Jul-2022 Release 1 allows attacker to launch arbitray activity and access senstive information. **CVE ID : CVE-2022-33685**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1837
Incorrect Authorization	12-Jul-2022	5.5	Improper authorization vulnerability in Knoxguard prior to SMR Jul-2022 Release 1 allows local attacker to disable keyguard and bypass Knoxguard lock by factory reset. **CVE ID : CVE-2022-33702**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1838
Time-of-check Time-of-use (TOCTOU) Race Condition	12-Jul-2022	4.7	A possible race condition vulnerability in score driver prior to SMR Jul-2022 Release 1 can allow local attackers to interleave malicious operations. **CVE ID : CVE-2022-33691**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1839
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, there is a possible out of bounds read due to a	https://corp.mediatek.com/product-	O-GOO-ANDR-210722/1840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	security-bulletin/July-2022	
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Improper access control vulnerability in updateLastConnectedClientInfo function of SemWifiApClient prior to SMR Jul-2022 Release 1 allows attacker to access wifi ap client mac address that connected. **CVE ID : CVE-2022-30750**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1841
Insertion of Sensitive Information into Log File	12-Jul-2022	3.3	Exposure of Sensitive Information in telephony-common.jar prior to SMR Jul-2022 Release 1 allows local attackers to access IMSI via log. **CVE ID : CVE-2022-33687**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1842
Insertion of Sensitive Information into Log File	12-Jul-2022	3.3	Sensitive information exposure vulnerability in EventType in SecTelephonyProvider prior to SMR Jul-	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2022 Release 1 allows local attackers with log access permission to get IMSI through device log. **CVE ID : CVE-2022-33688**		
Incorrect Permission Assignment for Critical Resource	12-Jul-2022	3.3	Improper access control vulnerability in TelephonyUI prior to SMR Jul-2022 Release 1 allows attackers to change preferred network type by unprotected binder call. **CVE ID : CVE-2022-33689**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1844
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Exposure of Sensitive Information in Messaging application prior to SMR Jul-2022 Release 1 allows local attacker to access imsi and iccid via log. **CVE ID : CVE-2022-33692**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1845
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Exposure of Sensitive Information in CSC application prior to SMR Jul-2022 Release 1 allows local attacker to access wifi information via unprotected intent broadcasting. **CVE ID : CVE-2022-33694**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1846
Exposure of Resource	12-Jul-2022	3.3	Improper access control vulnerability in	https://security.samsungmobile.com/securit	O-GOO-ANDR-210722/1847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			sendDHCPACKBroadcast function of SemWifiApClient prior to SMR Jul-2022 Release 1 allows attacker to access wifi ap client mac address that connected by using WIFI_AP_STA_STATE_CHANGED action. **CVE ID : CVE-2022-30752**	yUpdate.smsb?year=2022&month=7	
Insertion of Sensitive Information into Log File	12-Jul-2022	3.3	Sensitive information exposure vulnerability in ImsServiceSwitchBase in ImsCore prior to SMR Jul-2022 Release 1 allows local attackers with log access permission to get IMSI through device log. **CVE ID : CVE-2022-33697**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1848
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Improper access control vulnerability in sendDHCPACKBroadcast function of SemWifiApClient prior to SMR Jul-2022 Release 1 allows attacker to access wifi ap client mac address that connected by using WIFI_AP_STA_DHCPACK_EVENT action. **CVE ID : CVE-2022-30751**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inclusion of Functionality from Untrusted Control Sphere	12-Jul-2022	3.3	Improper access control vulnerability in KnoxCustomManager Service prior to SMR Jul-2022 Release 1 allows attacker to call PowerManaer.goToSleep method which is protected by system permission by sending braodcast intent. **CVE ID : CVE-2022-33701**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1850
Incorrect Authorization	12-Jul-2022	3.3	Improper authorization in isemtelephony prior to SMR Jul-2022 Release 1 allows attacker to obtain CID without ACCESS_FINE_LOCATION permission. **CVE ID : CVE-2022-30757**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1851
Incorrect Default Permissions	12-Jul-2022	3.3	Improper use of a unique device ID in unprotected SecSoterService prior to SMR Jul-2022 Release 1 allows local attackers to get the device ID without permission. **CVE ID : CVE-2022-30753**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1852
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Exposure of Sensitive Information in Telecom application prior to SMR Jul-2022 Release 1 allows local	https://security.samsungmobile.com/securityUpdate.smsb?	O-GOO-ANDR-210722/1853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to access ICCID via log. **CVE ID : CVE-2022-33698**	year=2022&month=7	
Files or Directories Accessible to External Parties	12-Jul-2022	2.3	Exposure of Sensitive Information in GsmAlarmManager prior to SMR Jul-2022 Release 1 allows local attacker to access iccid via log. **CVE ID : CVE-2022-33686**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1854
Insertion of Sensitive Information into Log File	12-Jul-2022	2.3	Exposure of Sensitive Information in CID Manager prior to SMR Jul-2022 Release 1 allows local attacker to access iccid via log. **CVE ID : CVE-2022-33693**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1855
Exposure of Resource to Wrong Sphere	12-Jul-2022	2.3	Exposure of Sensitive Information in getDsaSimImsi in TelephonyUI prior to SMR Jul-2022 Release 1 allows local attacker to access imsi via log. **CVE ID : CVE-2022-33699**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1856
Exposure of Resource to Wrong Sphere	12-Jul-2022	2.3	Exposure of Sensitive Information in putDsaSimImsi in TelephonyUI prior to SMR Jul-2022 Release 1 allows local attacker to access imsi via log. **CVE ID : CVE-2022-33700**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 12.0					
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784351; Issue ID: ALPS06784351. **CVE ID : CVE-2022-21768**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1858
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784430; Issue ID: ALPS06784430. **CVE ID : CVE-2022-21767**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1859
Improper Authentication	12-Jul-2022	7.8	Improper authentication vulnerability in AppLock prior to SMR Jul-2022 Release 1 allows attacker to bypass password confirm activity by	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hijacking the implicit intent. **CVE ID : CVE-2022-30755**		
N/A	12-Jul-2022	7.8	Implicit Intent hijacking vulnerability in AppLinker prior to SMR Jul-2022 Release 1 allow allows attackers to launch certain activities with privilege of AppLinker. **CVE ID : CVE-2022-30754**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1861
N/A	12-Jul-2022	7.8	Implicit Intent hijacking vulnerability in Finder prior to SMR Jul-2022 Release 1 allow allows attackers to launch certain activities with privilege of Finder. **CVE ID : CVE-2022-30756**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1862
Missing Authorization	06-Jul-2022	7.8	In Autoboot, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06713894; Issue ID: ALPS06713894.	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21777		
Improper Input Validation	12-Jul-2022	7.8	Improper validation vulnerability in ucmRetParcelable of KnoxSDK prior to SMR Jul-2022 Release 1 allows attackers to launch certain activities. **CVE ID : CVE-2022-33704**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1864
Incorrect Permission Assignment for Critical Resource	12-Jul-2022	7.8	Use of improper permission in InputManagerService prior to SMR Jul-2022 Release 1 allows unauthorized access to the service. **CVE ID : CVE-2022-33695**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1865
Improper Input Validation	12-Jul-2022	7.8	Improper validation vulnerability in CACertificateInfo prior to SMR Jul-2022 Release 1 allows attackers to launch certain activities. **CVE ID : CVE-2022-33703**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1866
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	7	In GPU, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07044730; Issue ID: ALPS07044730. **CVE ID : CVE-2022-20082**		
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641673. **CVE ID : CVE-2022-21765**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1868
Improper Input Validation	06-Jul-2022	6.7	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641653. **CVE ID : CVE-2022-21766**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1869
Improper Link Resolution Before File Access	06-Jul-2022	6.7	In sound driver, there is a possible information disclosure due to symlink following. This could lead to	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Link Following')			local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558663; Issue ID: ALPS06558663. **CVE ID : CVE-2022-21770**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In GED driver, 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: ALPS06641585; Issue ID: ALPS06641585. **CVE ID : CVE-2022-21771**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1871
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, there is a possible type confusion 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: ALPS06493842; Issue ID: ALPS06493842.	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21772		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641388; Issue ID: ALPS06641388. **CVE ID : CVE-2022-21773**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1873
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.7	In TEEI driver, 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: ALPS06641447; Issue ID: ALPS06641447. **CVE ID : CVE-2022-21774**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1874
Improper Locking	06-Jul-2022	6.7	In sched driver, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06479032; Issue ID: ALPS06479032. **CVE ID : CVE-2022-21775**		
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704393. **CVE ID : CVE-2022-21779**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1876
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704526. **CVE ID : CVE-2022-21780**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704433. **CVE ID : CVE-2022-21781**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1878
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704508. **CVE ID : CVE-2022-21782**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1879
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06704526; Issue ID: ALPS06704482. **CVE ID : CVE-2022-21783**		
Improper Input Validation	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06704526; Issue ID: ALPS06704462. **CVE ID : CVE-2022-21784**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1881
Out-of-bounds Write	06-Jul-2022	6.7	In WLAN driver, 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: ALPS06807363; Issue ID: ALPS06807363. **CVE ID : CVE-2022-21785**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1882
Incorrect Type Conversion or Cast	06-Jul-2022	6.7	In audio DSP, there is a possible memory corruption due to improper casting. This could lead to	https://corp.mediatek.com/product-security-	O-GOO-ANDR-210722/1883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06558822; Issue ID: ALPS06558822. **CVE ID : CVE-2022-21786**	bulletin/July-2022	
Out-of-bounds Write	06-Jul-2022	6.7	In audio DSP, 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: ALPS06558844; Issue ID: ALPS06558844. **CVE ID : CVE-2022-21787**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1884
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jul-2022	6.4	In MDP, 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: ALPS06545450; Issue ID: ALPS06545450.	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21776		
N/A	12-Jul-2022	5.5	Unprotected dynamic receiver in Wearable Manager Service prior to SMR Jul-2022 Release 1 allows attacker to launch arbitray activity and access senstive information. **CVE ID : CVE-2022-33685**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1886
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044708. **CVE ID : CVE-2022-21763**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1887
Missing Authorization	06-Jul-2022	5.5	In telecom service, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07044717; Issue ID: ALPS07044717. **CVE ID : CVE-2022-21764**		
Incorrect Authorization	12-Jul-2022	5.5	Improper authorization vulnerability in Knoxguard prior to SMR Jul-2022 Release 1 allows local attacker to disable keyguard and bypass Knoxguard lock by factory reset. **CVE ID : CVE-2022-33702**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1889
Incorrect Default Permissions	12-Jul-2022	5.5	Implicit Intent hijacking vulnerability in Finder prior to SMR Jul-2022 Release 1 allow allows attackers to access some protected information with privilege of Finder. **CVE ID : CVE-2022-30758**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1890
Time-of-check Time-of-use (TOCTOU) Race Condition	12-Jul-2022	4.7	A possible race condition vulnerability in score driver prior to SMR Jul-2022 Release 1 can allow local attackers to interleave malicious operations. **CVE ID : CVE-2022-33691**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jul-2022	4.4	In CCCI, 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: ALPS06641673; Issue ID: ALPS06641687. **CVE ID : CVE-2022-21769**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1892
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Improper access control vulnerability in sendDHCPACKBroadcast function of SemWifiApClient prior to SMR Jul-2022 Release 1 allows attacker to access wifi ap client mac address that connected by using WIFI_AP_STA_STATE_CHANGED action. **CVE ID : CVE-2022-30752**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1893
Incorrect Default Permissions	12-Jul-2022	3.3	Improper use of a unique device ID in unprotected SecSoterService prior to SMR Jul-2022 Release 1 allows local attackers to get the device ID without permission.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30753		
Insertion of Sensitive Information into Log File	12-Jul-2022	3.3	Exposure of Sensitive Information in telephony-common.jar prior to SMR Jul-2022 Release 1 allows local attackers to access IMSI via log. **CVE ID : CVE-2022-33687**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1895
Insertion of Sensitive Information into Log File	12-Jul-2022	3.3	Sensitive information exposure vulnerability in EventType in SecTelephonyProvider prior to SMR Jul-2022 Release 1 allows local attackers with log access permission to get IMSI through device log. **CVE ID : CVE-2022-33688**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1896
Incorrect Permission Assignment for Critical Resource	12-Jul-2022	3.3	Improper access control vulnerability in TelephonyUI prior to SMR Jul-2022 Release 1 allows attackers to change preferred network type by unprotected binder call. **CVE ID : CVE-2022-33689**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1897
Improper Limitation of a Pathname to a Restricted	12-Jul-2022	3.3	Improper input validation in Contacts Storage prior to SMR Jul-2022 Release 1	https://security.samsungmobile.com/securityUpdate.smsb?	O-GOO-ANDR-210722/1898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			allows attacker to access arbitrary file. **CVE ID : CVE-2022-33690**	year=2022&month=7	
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Improper access control vulnerability in sendDHCPACKBroadcast function of SemWifiApClient prior to SMR Jul-2022 Release 1 allows attacker to access wifi ap client mac address that connected by using WIFI_AP_STA_DHCPACK_EVENT action. **CVE ID : CVE-2022-30751**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1899
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Exposure of Sensitive Information in CSC application prior to SMR Jul-2022 Release 1 allows local attacker to access wifi information via unprotected intent broadcasting. **CVE ID : CVE-2022-33694**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1900
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Improper access control vulnerability in updateLastConnectedClientInfo function of SemWifiApClient prior to SMR Jul-2022 Release 1 allows attacker to access wifi ap client mac address that connected.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30750		
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Exposure of Sensitive Information in Telephony service prior to SMR Jul-2022 Release 1 allows local attacker to access imsi and iccid via log. **CVE ID : CVE-2022-33696**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1902
Insertion of Sensitive Information into Log File	12-Jul-2022	3.3	Sensitive information exposure vulnerability in ImsServiceSwitchBase in ImsCore prior to SMR Jul-2022 Release 1 allows local attackers with log access permission to get IMSI through device log. **CVE ID : CVE-2022-33697**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1903
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Exposure of Sensitive Information in Messaging application prior to SMR Jul-2022 Release 1 allows local attacker to access imsi and iccid via log. **CVE ID : CVE-2022-33692**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1904
Inclusion of Functionality from Untrusted Control Sphere	12-Jul-2022	3.3	Improper access control vulnerability in KnoxCustomManagerService prior to SMR Jul-2022 Release 1 allows attacker to call PowerManaer.goToSleep method which is	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected by system permission by sending braodcast intent. **CVE ID : CVE-2022-33701**		
Incorrect Authorization	12-Jul-2022	3.3	Improper authorization in isemtelephony prior to SMR Jul-2022 Release 1 allows attacker to obtain CID without ACCESS_FINE_LOCATION permission. **CVE ID : CVE-2022-30757**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1906
Exposure of Resource to Wrong Sphere	12-Jul-2022	3.3	Exposure of Sensitive Information in Telecom application prior to SMR Jul-2022 Release 1 allows local attackers to access ICCID via log. **CVE ID : CVE-2022-33698**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1907
Files or Directories Accessible to External Parties	12-Jul-2022	2.3	Exposure of Sensitive Information in GsmAlarmManager prior to SMR Jul-2022 Release 1 allows local attacker to access iccid via log. **CVE ID : CVE-2022-33686**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1908
Insertion of Sensitive Information into Log File	12-Jul-2022	2.3	Exposure of Sensitive Information in CID Manager prior to SMR Jul-2022 Release 1 allows local attacker to access iccid via log.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33693		
Exposure of Resource to Wrong Sphere	12-Jul-2022	2.3	Exposure of Sensitive Information in getDsaSimImsi in TelephonyUI prior to SMR Jul-2022 Release 1 allows local attacker to access imsi via log. **CVE ID : CVE-2022-33699**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1910
Exposure of Resource to Wrong Sphere	12-Jul-2022	2.3	Exposure of Sensitive Information in putDsaSimImsi in TelephonyUI prior to SMR Jul-2022 Release 1 allows local attacker to access imsi via log. **CVE ID : CVE-2022-33700**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7	O-GOO-ANDR-210722/1911
Affected Version(s): 8.1					
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784430; Issue ID: ALPS06784430. **CVE ID : CVE-2022-21767**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784351; Issue ID: ALPS06784351. **CVE ID : CVE-2022-21768**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1913
Affected Version(s): 9.0					
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06784430; Issue ID: ALPS06784430. **CVE ID : CVE-2022-21767**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1914
Out-of-bounds Write	06-Jul-2022	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2022	O-GOO-ANDR-210722/1915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS06784351; Issue ID: ALPS06784351. **CVE ID : CVE-2022-21768**		
Vendor: H3C					
Product: magic_r100_firmware					
Affected Version(s): v100r005					
N/A	06-Jul-2022	9.8	The udpserver in H3C Magic R100 V200R004 and V100R005 has the 9034 port opened, allowing attackers to execute arbitrary commands. **CVE ID : CVE-2022-34598**	N/A	O-H3C-MAGI-210722/1916
Affected Version(s): v200r004					
N/A	06-Jul-2022	9.8	The udpserver in H3C Magic R100 V200R004 and V100R005 has the 9034 port opened, allowing attackers to execute arbitrary commands. **CVE ID : CVE-2022-34598**	N/A	O-H3C-MAGI-210722/1917
Vendor: hpe					
Product: flexfabric_5945_firmware					
Affected Version(s): 7.10.r6635					
Improper Neutralization of Input During	08-Jul-2022	4.8	A potential security vulnerability has been identified in certain HPE FlexNetwork and FlexFabric switch	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&doc	O-HPE-FLEX-210722/1918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			products. The vulnerability could be remotely exploited to allow cross site scripting (XSS). HPE has made the following software updates to resolve the vulnerability. HPE FlexNetwork 5130EL_7.10.R3507P02 and HPE FlexFabric 5945_7.10.R6635. **CVE ID : CVE-2022-28624**	Id=emr_na-hpesbnw04265en_us	
Product: flexnetwork_5130_ei_firmware					
Affected Version(s): 7.10.r3507p02					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2022	4.8	A potential security vulnerability has been identified in certain HPE FlexNetwork and FlexFabric switch products. The vulnerability could be remotely exploited to allow cross site scripting (XSS). HPE has made the following software updates to resolve the vulnerability. HPE FlexNetwork 5130EL_7.10.R3507P02 and HPE FlexFabric 5945_7.10.R6635. **CVE ID : CVE-2022-28624**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04265en_us	O-HPE-FLEX-210722/1919
Vendor: IBM					
Product: aix					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Missing Authorization	01-Jul-2022	5.4	An improper validation vulnerability in IBM InfoSphere Information Server 11.7 Pack for SAP Apps and BW Packs may lead to creation of directories and files on the server file system that may contain non-sensitive debugging information like stack traces. IBM X-Force ID: 221323. **CVE ID : CVE-2022-22373**	https://exchange.xforce.ibmcloud.com/vulnerabilities/221323, https://www.ibm.com/support/pages/node/6600235	O-IBM-AIX-210722/1920
Vendor: Kddi					
Product: home_spot_cube_2_firmware					
Affected Version(s): * Up to (including) v102					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Jul-2022	8.8	HOME SPOT CUBE2 V102 contains an OS command injection vulnerability due to improper processing of data received from DHCP server. An adjacent attacker may execute an arbitrary OS command on the product if a malicious DHCP server is placed on the WAN side of the product. **CVE ID : CVE-2022-33948**	https://www.au.com/support/service/mobile/guide/wlan/home_spot_cube_2/	O-KDD-HOME-210722/1921
Vendor: Linux					
Product: linux_kernel					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Exposure of Sensitive Information to an Unauthorized Actor	05-Jul-2022	7.1	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742). **CVE ID : CVE-2022-26365**	https://xenbits.xenproject.org/xsa/advisory-403.txt, http://xenbits.xen.org/xsa/advisory-403.html, http://www.openwall.com/lists/oss-security/2022/07/05/6	O-LIN-LINU-210722/1922
Exposure of Sensitive Information to an Unauthorized Actor	05-Jul-2022	7.1	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which	https://xenbits.xenproject.org/xsa/advisory-403.txt, http://xenbits.xen.org/xsa/advisory-403.html, http://www.o	O-LIN-LINU-210722/1923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742). **CVE ID : CVE-2022-33740**	penwall.com/lists/oss-security/2022/07/05/6	
Exposure of Sensitive Information to an Unauthorized Actor	05-Jul-2022	7.1	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the	https://xenbits.xenproject.org/xsa/advisory-403.txt, http://xenbits.xen.org/xsa/advisory-403.html, http://www.openwall.com/lists/oss-security/2022/07/05/6	O-LIN-LINU-210722/1924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742). **CVE ID : CVE-2022-33741**		
Exposure of Sensitive Information to an Unauthorized Actor	05-Jul-2022	7.1	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-	https://xenbits.xenproject.org/xsa/advisory-403.txt, http://xenbits.xen.org/xsa/advisory-403.html, http://www.openwall.com/lists/oss-security/2022/07/05/6	O-LIN-LINU-210722/1925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			33741, CVE-2022-33742). **CVE ID : CVE-2022-33742**		
Missing Authorization	01-Jul-2022	5.4	An improper validation vulnerability in IBM InfoSphere Information Server 11.7 Pack for SAP Apps and BW Packs may lead to creation of directories and files on the server file system that may contain non-sensitive debugging information like stack traces. IBM X-Force ID: 221323. **CVE ID : CVE-2022-22373**	https://exchange.xforce.ibmcloud.com/vulnerabilities/221323, https://www.ibm.com/support/pages/node/6600235	O-LIN-LINU-210722/1926
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Jul-2022	5.4	IBM CICS TX Standard and Advanced 11.1 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 229330. **CVE ID : CVE-2022-34160**	https://www.ibm.com/support/pages/node/6601555, https://www.ibm.com/support/pages/node/6601553, https://exchange.xforce.ibmcloud.com/vulnerabilities/229330	O-LIN-LINU-210722/1927
Improper Neutralization of Input During	08-Jul-2022	5.4	IBM CICS TX Standard and Advanced 11.1 is vulnerable to cross-site scripting. This vulnerability allows	https://www.ibm.com/support/pages/node/6601609, https://www.i	O-LIN-LINU-210722/1928

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: 229430. **CVE ID : CVE-2022-34166**	bm.com/support/pages/node/6601579	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2022	5.4	IBM CICS TX Standard and Advanced 11.1 is vulnerable to stored 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: 229432. **CVE ID : CVE-2022-34167**	https://www.ibm.com/support/pages/node/6601655, https://exchange.xforce.ibmcloud.com/vulnerabilities/229432, https://www.ibm.com/support/pages/node/6601657	O-LIN-LINU-210722/1929
Improper Neutralization of Special Elements in Output Used by a Downstream Component	08-Jul-2022	5.4	IBM CICS TX Standard and Advanced 11.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting,	https://exchange.xforce.ibmcloud.com/vulnerabilities/229435, https://www.ibm.com/support/pages/node/6601663, https://www.ibm.com/suppo	O-LIN-LINU-210722/1930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			cache poisoning or session hijacking. IBM X-Force ID: 229435. **CVE ID : CVE-2022-34306**	rt/pages/node/6601659	
Affected Version(s): * Up to (excluding) 5.19					
Use After Free	06-Jul-2022	5.5	There are use-after-free vulnerabilities caused by timer handler in net/rose/rose_timer.c of linux that allow attackers to crash linux kernel without any privileges. **CVE ID : CVE-2022-2318**	https://github.com/torvalds/linux/commit/9cc02ede696272c5271a401e4f27c262359bc2f6	O-LIN-LINU-210722/1931
Affected Version(s): 5.19					
Use After Free	06-Jul-2022	5.5	There are use-after-free vulnerabilities caused by timer handler in net/rose/rose_timer.c of linux that allow attackers to crash linux kernel without any privileges. **CVE ID : CVE-2022-2318**	https://github.com/torvalds/linux/commit/9cc02ede696272c5271a401e4f27c262359bc2f6	O-LIN-LINU-210722/1932
Affected Version(s): From (including) 3.13 Up to (including) 5.18					
N/A	05-Jul-2022	4.7	Arm guests can cause Dom0 DoS via PV devices When mapping pages of guests on Arm, dom0 is using an rbtree to keep track of the foreign mappings. Updating of that rbtree is not always done completely with	https://xenbits.xenproject.org/xsa/advisory-406.txt, http://xenbits.xen.org/xsa/advisory-406.html, http://www.openwall.com/lists/oss-	O-LIN-LINU-210722/1933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the related lock held, resulting in a small race window, which can be used by unprivileged guests via PV devices to cause inconsistencies of the rbtree. These inconsistencies can lead to Denial of Service (DoS) of dom0, e.g. by causing crashes or the inability to perform further mappings of other guests' memory pages. **CVE ID : CVE-2022-33744**	security/2022/07/05/4	
Affected Version(s): From (including) 5.8.0 Up to (including) 5.18.9					
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2022	7.8	An issue was discovered in the Linux kernel through 5.18.9. A type confusion bug in nft_set_elem_init (leading to a buffer overflow) could be used by a local attacker to escalate privileges, a different vulnerability than CVE-2022-32250. (The attacker can obtain root access, but must start with an unprivileged user namespace to obtain CAP_NET_ADMIN access.) This can be fixed in nft_setelem_parse_data in	https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?id=7e6bc1f6cabcd30aba0b11219d8e01b952eacbb6, https://lore.kernel.org/netfilter-devel/cd9428b6-7ffb-dd22-d949-d86f4869f452@randorisec.fr/T/#u	O-LIN-LINU-210722/1934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/netfilter/nf_tables_api.c. **CVE ID : CVE-2022-34918**		
Affected Version(s): From (including) 5.9 Up to (including) 5.18					
N/A	05-Jul-2022	7.8	network backend may cause Linux netfront to use freed SKBs While adding logic to support XDP (eXpress Data Path), a code label was moved in a way allowing for SKBs having references (pointers) retained for further processing to nevertheless be freed. **CVE ID : CVE-2022-33743**	https://xenbits.xenproject.org/xsa/advisory-405.txt, http://xenbits.xen.org/xsa/advisory-405.html, http://www.openwall.com/lists/oss-security/2022/07/05/5	O-LIN-LINU-210722/1935
Vendor: mediatek					
Product: lr11					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883.	https://corp.mediatek.com/product-security-bulletin/July-2022	O-MED-LR11-210722/1936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20083		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-MED-LR11-210722/1937
Product: lr12					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883;	https://corp.mediatek.com/product-security-bulletin/July-2022	O-MED-LR12-210722/1938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-MED-LR12-210722/1939
Product: lr12a					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/July-2022	O-MED-LR12-210722/1940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-MED-LR12-210722/1941
Product: lr13					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2022	O-MED-LR13-210722/1942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-MED-LR13-210722/1943
Product: lr9					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/July-2022	O-MED-LR9-210722/1944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-MED-LR9-210722/1945
Product: nr15					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2022	O-MED-NR15-210722/1946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-MED-NR15-210722/1947
Product: nr16					
Affected Version(s): -					
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G/3G CC, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding combined FACILITY with no additional execution	https://corp.mediatek.com/product-security-bulletin/July-2022	O-MED-NR16-210722/1948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00803883; Issue ID: MOLY00803883. **CVE ID : CVE-2022-20083**		
Out-of-bounds Write	06-Jul-2022	9.8	In Modem 2G RR, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell Data (PNCD) improper neighbouring cell size with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00810064; Issue ID: ALPS06641626. **CVE ID : CVE-2022-21744**	https://corp.mediatek.com/product-security-bulletin/July-2022	O-MED-NR16-210722/1949
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Improper Privilege Management	06-Jul-2022	7.8	A local privilege escalation (LPE) issue was discovered in the ransomware canaries features of Elastic Endpoint Security for Windows, which could allow	https://discuss.elastic.co/t/elastic-8-3-1-8-3-0-and-7-17-5-security-update/308613, https://www.e	O-MIC-WIND-210722/1950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unprivileged users to elevate their privileges to those of the LocalSystem account. **CVE ID : CVE-2022-23714**	lastic.co/community/security	
Unprotected Storage of Credentials	11-Jul-2022	5.5	The CODESYS OPC DA Server prior V3.5.18.20 stores PLC passwords as plain text in its configuration file so that it is visible to all authorized Microsoft Windows users of the system. **CVE ID : CVE-2022-1794**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17129&token=1c1485c4a700c04f2069699f5be7558d276ca117&download=	O-MIC-WIND-210722/1951
Missing Authorization	01-Jul-2022	5.4	An improper validation vulnerability in IBM InfoSphere Information Server 11.7 Pack for SAP Apps and BW Packs may lead to creation of directories and files on the server file system that may contain non-sensitive debugging information like stack traces. IBM X-Force ID: 221323. **CVE ID : CVE-2022-22373**	https://exchange.xforce.ibmcloud.com/vulnerabilities/221323, https://www.ibm.com/support/pages/node/6600235	O-MIC-WIND-210722/1952
Product: windows_10					
Affected Version(s): -					
Improper Privilege	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege	https://portal.msrc.microsoft	O-MIC-WIND-210722/1953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Vulnerability. This CVE ID is unique from CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	.com/en-US/security-guidance/advisory/CVE-2022-22026	
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22038	O-MIC-WIND-210722/1954
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/1955
Improper Privilege Management	12-Jul-2022	7.8	Windows Credential Guard Domain-joined Public Key Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22031	O-MIC-WIND-210722/1956
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/1957
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210722/1958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ory/CVE-2022-22043	
Improper Privilege Management	12-Jul-2022	7.8	Windows.Devices.Picker.dll Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22045	O-MIC-WIND-210722/1959
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/1960
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/1961
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/1962
Improper Privilege Management	12-Jul-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-30206, CVE-2022-30226.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22041	O-MIC-WIND-210722/1963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22041		
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036	O-MIC-WIND-210722/1964
Exposure of Resource to Wrong Sphere	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30223. **CVE ID : CVE-2022-22042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042	O-MIC-WIND-210722/1965
Affected Version(s): 1607					
Improper Privilege Management	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22026	O-MIC-WIND-210722/1966
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22038	O-MIC-WIND-210722/1967
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/1968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22024		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/1969
Improper Privilege Management	12-Jul-2022	7.8	Windows Credential Guard Domain-joined Public Key Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22031	O-MIC-WIND-210722/1970
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/1971
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22043	O-MIC-WIND-210722/1972
Improper Privilege Management	12-Jul-2022	7.8	Windows.Devices.Picker.dll Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22045	O-MIC-WIND-210722/1973
Improper Privilege	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210722/1974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	US/security-guidance/advisory/CVE-2022-22047	
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025	O-MIC-WIND-210722/1975
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/1976
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/1977
Improper Privilege Management	12-Jul-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22041	O-MIC-WIND-210722/1978
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210722/1979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22022**	US/security-guidance/advisory/CVE-2022-22022	
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036	O-MIC-WIND-210722/1980
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023	O-MIC-WIND-210722/1981
Exposure of Resource to Wrong Sphere	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30223. **CVE ID : CVE-2022-22042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042	O-MIC-WIND-210722/1982
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/1983
Affected Version(s): 1809					
Improper Privilege	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-210722/1984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	guidance/advisory/CVE-2022-22026	
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22038	O-MIC-WIND-210722/1985
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027. **CVE ID : CVE-2022-22024**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/1986
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/1987
Improper Privilege Management	12-Jul-2022	7.8	Windows Credential Guard Domain-joined Public Key Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22031	O-MIC-WIND-210722/1988
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/1989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22043	O-MIC-WIND-210722/1990
Improper Privilege Management	12-Jul-2022	7.8	Windows.Devices.Picker.dll Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22045	O-MIC-WIND-210722/1991
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/1992
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025	O-MIC-WIND-210722/1993
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/1994
Uncontrolled Resource	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210722/1995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	US/security-guidance/advisory/CVE-2022-22040	
Improper Privilege Management	12-Jul-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22041	O-MIC-WIND-210722/1996
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22022	O-MIC-WIND-210722/1997
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036	O-MIC-WIND-210722/1998
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023	O-MIC-WIND-210722/1999
Exposure of Resource	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210722/2000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			Vulnerability. This CVE ID is unique from CVE-2022-30223. **CVE ID : CVE-2022-22042**	US/security-guidance/advisory/CVE-2022-22042	
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/2001
Affected Version(s): 20h2					
Improper Privilege Management	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22026	O-MIC-WIND-210722/2002
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22038	O-MIC-WIND-210722/2003
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027. **CVE ID : CVE-2022-22024**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/2004
Improper Control of Generation of Code	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210722/2005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	ory/CVE-2022-22027	
Improper Privilege Management	12-Jul-2022	7.8	Windows Credential Guard Domain-joined Public Key Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22031	O-MIC-WIND-210722/2006
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/2007
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22043	O-MIC-WIND-210722/2008
Improper Privilege Management	12-Jul-2022	7.8	Windows.Devices.Picker.dll Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22045	O-MIC-WIND-210722/2009
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/2010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025	O-MIC-WIND-210722/2011
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/2012
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/2013
Improper Privilege Management	12-Jul-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22041	O-MIC-WIND-210722/2014
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22022	O-MIC-WIND-210722/2015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22022		
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036	O-MIC-WIND-210722/2016
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023	O-MIC-WIND-210722/2017
Exposure of Resource to Wrong Sphere	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30223. **CVE ID : CVE-2022-22042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042	O-MIC-WIND-210722/2018
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/2019
Affected Version(s): 21h1					
Improper Privilege Management	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22026	O-MIC-WIND-210722/2020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22038	O-MIC-WIND-210722/2021
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027. **CVE ID : CVE-2022-22024**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/2022
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/2023
Improper Privilege Management	12-Jul-2022	7.8	Windows Credential Guard Domain-joined Public Key Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22031	O-MIC-WIND-210722/2024
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/2025
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-210722/2026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22043	guidance/advisory/CVE-2022-22043	
Improper Privilege Management	12-Jul-2022	7.8	Windows.Devices.Picker.dll Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22045	O-MIC-WIND-210722/2027
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/2028
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025	O-MIC-WIND-210722/2029
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/2030
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/2031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jul-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22041	O-MIC-WIND-210722/2032
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22022	O-MIC-WIND-210722/2033
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036	O-MIC-WIND-210722/2034
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023	O-MIC-WIND-210722/2035
Exposure of Resource to Wrong Sphere	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30223.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042	O-MIC-WIND-210722/2036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22042		
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/2037
Affected Version(s): 21h2					
Improper Privilege Management	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22026	O-MIC-WIND-210722/2038
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22038	O-MIC-WIND-210722/2039
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027. **CVE ID : CVE-2022-22024**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/2040
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/2041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jul-2022	7.8	Windows Credential Guard Domain-joined Public Key Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22031	O-MIC-WIND-210722/2042
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/2043
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22043	O-MIC-WIND-210722/2044
Improper Privilege Management	12-Jul-2022	7.8	Windows.Devices.Picker.dll Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22045	O-MIC-WIND-210722/2045
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/2046
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210722/2047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22025	ory/CVE-2022-22025	
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/2048
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/2049
Improper Privilege Management	12-Jul-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22041	O-MIC-WIND-210722/2050
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22022	O-MIC-WIND-210722/2051
Improper Privilege	12-Jul-2022	7	Performance Counters for Windows Elevation of	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210722/2052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Privilege Vulnerability. **CVE ID : CVE-2022-22036**	US/security-guidance/advisory/CVE-2022-22036	
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023	O-MIC-WIND-210722/2053
Exposure of Resource to Wrong Sphere	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30223. **CVE ID : CVE-2022-22042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042	O-MIC-WIND-210722/2054
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/2055
Product: windows_11					
Affected Version(s): -					
Improper Privilege Management	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22026	O-MIC-WIND-210722/2056
Improper Control of Generation of Code	12-Jul-2022	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-210722/2057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			**CVE ID : CVE-2022-22038**	guidance/advisory/CVE-2022-22038	
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027. **CVE ID : CVE-2022-22024**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/2058
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/2059
Improper Privilege Management	12-Jul-2022	7.8	Windows Credential Guard Domain-joined Public Key Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22031	O-MIC-WIND-210722/2060
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/2061
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22043	O-MIC-WIND-210722/2062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jul-2022	7.8	Windows.Devices.Picker.dll Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22045	O-MIC-WIND-210722/2063
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/2064
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025	O-MIC-WIND-210722/2065
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/2066
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/2067
Improper Privilege	12-Jul-2022	7.2	Windows Print Spooler Elevation of Privilege	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210722/2068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22041**	US/security-guidance/advisory/CVE-2022-22041	
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22022	O-MIC-WIND-210722/2069
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036	O-MIC-WIND-210722/2070
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023	O-MIC-WIND-210722/2071
Exposure of Resource to Wrong Sphere	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30223. **CVE ID : CVE-2022-22042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042	O-MIC-WIND-210722/2072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/2073
Product: windows_7					
Affected Version(s): -					
Improper Privilege Management	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22026	O-MIC-WIND-210722/2074
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027. **CVE ID : CVE-2022-22024**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/2075
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/2076
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/2077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22043	O-MIC-WIND-210722/2078
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/2079
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025	O-MIC-WIND-210722/2080
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/2081
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/2082
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210722/2083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22022**	US/security-guidance/advisory/CVE-2022-22022	
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036	O-MIC-WIND-210722/2084
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023	O-MIC-WIND-210722/2085
Exposure of Resource to Wrong Sphere	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30223. **CVE ID : CVE-2022-22042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042	O-MIC-WIND-210722/2086
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/2087
Product: windows_8.1					
Affected Version(s): -					
Improper Privilege	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege	https://portal.msrc.microsoft	O-MIC-WIND-210722/2088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Vulnerability. This CVE ID is unique from CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	.com/en-US/security-guidance/advisory/CVE-2022-22026	
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22038	O-MIC-WIND-210722/2089
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027. **CVE ID : CVE-2022-22024**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/2090
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/2091
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/2092
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210722/2093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22043	ory/CVE-2022-22043	
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/2094
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025	O-MIC-WIND-210722/2095
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/2096
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/2097
Improper Privilege Management	12-Jul-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-30206, CVE-2022-30226.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22041	O-MIC-WIND-210722/2098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22041		
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22022	O-MIC-WIND-210722/2099
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036	O-MIC-WIND-210722/2100
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023	O-MIC-WIND-210722/2101
Exposure of Resource to Wrong Sphere	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30223. **CVE ID : CVE-2022-22042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042	O-MIC-WIND-210722/2102
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/2103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: windows_rt_8.1					
Affected Version(s): -					
Improper Privilege Management	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22026	O-MIC-WIND-210722/2104
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22038	O-MIC-WIND-210722/2105
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027. **CVE ID : CVE-2022-22024**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/2106
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/2107
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/2108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22043	O-MIC-WIND-210722/2109
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/2110
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025	O-MIC-WIND-210722/2111
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/2112
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/2113
Improper Privilege	12-Jul-2022	7.2	Windows Print Spooler Elevation of Privilege	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210722/2114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22041**	US/security-guidance/advisory/CVE-2022-22041	
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22022	O-MIC-WIND-210722/2115
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036	O-MIC-WIND-210722/2116
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023	O-MIC-WIND-210722/2117
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/2118
Product: windows_server_2008					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22026	O-MIC-WIND-210722/2119
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Windows Network File System Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22039. **CVE ID : CVE-2022-22029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22029	O-MIC-WIND-210722/2120
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027. **CVE ID : CVE-2022-22024**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/2121
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/2122
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/2123
Improper Privilege	12-Jul-2022	7.8	Windows Fast FAT File System Driver	https://portal.msrc.microsoft	O-MIC-WIND-210722/2124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22043**	.com/en-US/security-guidance/advisory/CVE-2022-22043	
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/2125
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025	O-MIC-WIND-210722/2126
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/2127
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.5	Windows Network File System Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22029. **CVE ID : CVE-2022-22039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22039	O-MIC-WIND-210722/2128
Uncontrolled Resource	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-210722/2129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	guidance/advisory/CVE-2022-22040	
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22022	O-MIC-WIND-210722/2130
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023	O-MIC-WIND-210722/2131
Exposure of Resource to Wrong Sphere	12-Jul-2022	5.9	Windows Network File System Information Disclosure Vulnerability. **CVE ID : CVE-2022-22028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22028	O-MIC-WIND-210722/2132
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/2133
Affected Version(s): r2					
Improper Privilege Management	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210722/2134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	ory/CVE-2022-22026	
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Windows Network File System Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22039. **CVE ID : CVE-2022-22029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22029	O-MIC-WIND-210722/2135
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027. **CVE ID : CVE-2022-22024**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/2136
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/2137
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/2138
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210722/2139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22043	ory/CVE-2022-22043	
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/2140
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025	O-MIC-WIND-210722/2141
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/2142
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.5	Windows Network File System Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22029. **CVE ID : CVE-2022-22039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22039	O-MIC-WIND-210722/2143
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/2144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22040		
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22022	O-MIC-WIND-210722/2145
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036	O-MIC-WIND-210722/2146
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023	O-MIC-WIND-210722/2147
Exposure of Resource to Wrong Sphere	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30223. **CVE ID : CVE-2022-22042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042	O-MIC-WIND-210722/2148
Exposure of Resource to Wrong Sphere	12-Jul-2022	5.9	Windows Network File System Information Disclosure Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22028	O-MIC-WIND-210722/2149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22028		
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/2150
Product: windows_server_2012					
Affected Version(s): -					
Improper Privilege Management	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22026	O-MIC-WIND-210722/2151
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Windows Network File System Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22039. **CVE ID : CVE-2022-22029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22029	O-MIC-WIND-210722/2152
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22038	O-MIC-WIND-210722/2153
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/2154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22024		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/2155
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/2156
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22043	O-MIC-WIND-210722/2157
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/2158
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025	O-MIC-WIND-210722/2159
Improper Privilege	12-Jul-2022	7.5	Windows Advanced Local Procedure Call	https://portal.msrc.microsoft	O-MIC-WIND-210722/2160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	.com/en-US/security-guidance/advisory/CVE-2022-22037	
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.5	Windows Network File System Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22029. **CVE ID : CVE-2022-22039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22039	O-MIC-WIND-210722/2161
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/2162
Improper Privilege Management	12-Jul-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22041	O-MIC-WIND-210722/2163
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22022	O-MIC-WIND-210722/2164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22022		
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036	O-MIC-WIND-210722/2165
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023	O-MIC-WIND-210722/2166
Exposure of Resource to Wrong Sphere	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30223. **CVE ID : CVE-2022-22042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042	O-MIC-WIND-210722/2167
Exposure of Resource to Wrong Sphere	12-Jul-2022	5.9	Windows Network File System Information Disclosure Vulnerability. **CVE ID : CVE-2022-22028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22028	O-MIC-WIND-210722/2168
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/2169
Affected Version(s): r2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22026	O-MIC-WIND-210722/2170
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Windows Network File System Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22039. **CVE ID : CVE-2022-22029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22029	O-MIC-WIND-210722/2171
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22038	O-MIC-WIND-210722/2172
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027. **CVE ID : CVE-2022-22024**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/2173
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/2174
Improper Privilege	12-Jul-2022	7.8	Windows Graphics Component Elevation	https://portal.msrc.microsoft	O-MIC-WIND-210722/2175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	.com/en-US/security-guidance/advisory/CVE-2022-22034	
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22043	O-MIC-WIND-210722/2176
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/2177
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025	O-MIC-WIND-210722/2178
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/2179
Improper Control of Generation of Code	12-Jul-2022	7.5	Windows Network File System Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210722/2180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			CVE ID is unique from CVE-2022-22029. **CVE ID : CVE-2022-22039**	ory/CVE-2022-22039	
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/2181
Improper Privilege Management	12-Jul-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22041	O-MIC-WIND-210722/2182
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22022	O-MIC-WIND-210722/2183
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036	O-MIC-WIND-210722/2184
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210722/2185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	US/security-guidance/advisory/CVE-2022-22023	
Exposure of Resource to Wrong Sphere	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30223. **CVE ID : CVE-2022-22042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042	O-MIC-WIND-210722/2186
Exposure of Resource to Wrong Sphere	12-Jul-2022	5.9	Windows Network File System Information Disclosure Vulnerability. **CVE ID : CVE-2022-22028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22028	O-MIC-WIND-210722/2187
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/2188
Product: windows_server_2016					
Affected Version(s): -					
Improper Privilege Management	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22026	O-MIC-WIND-210722/2189
Improper Control of Generation of Code	12-Jul-2022	8.1	Windows Network File System Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-210722/2190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			CVE ID is unique from CVE-2022-22039. **CVE ID : CVE-2022-22029**	guidance/advisory/CVE-2022-22029	
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22038	O-MIC-WIND-210722/2191
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027. **CVE ID : CVE-2022-22024**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/2192
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/2193
Improper Privilege Management	12-Jul-2022	7.8	Windows Credential Guard Domain-joined Public Key Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22031	O-MIC-WIND-210722/2194
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/2195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22043	O-MIC-WIND-210722/2196
Improper Privilege Management	12-Jul-2022	7.8	Windows.Devices.Picker.dll Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22045	O-MIC-WIND-210722/2197
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/2198
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025	O-MIC-WIND-210722/2199
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/2200
Improper Control of Generation	12-Jul-2022	7.5	Windows Network File System Remote Code Execution	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210722/2201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			Vulnerability. This CVE ID is unique from CVE-2022-22029. **CVE ID : CVE-2022-22039**	US/security-guidance/advisory/CVE-2022-22039	
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/2202
Improper Privilege Management	12-Jul-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22041	O-MIC-WIND-210722/2203
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22022	O-MIC-WIND-210722/2204
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036	O-MIC-WIND-210722/2205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023	O-MIC-WIND-210722/2206
Exposure of Resource to Wrong Sphere	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30223. **CVE ID : CVE-2022-22042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042	O-MIC-WIND-210722/2207
Exposure of Resource to Wrong Sphere	12-Jul-2022	5.9	Windows Network File System Information Disclosure Vulnerability. **CVE ID : CVE-2022-22028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22028	O-MIC-WIND-210722/2208
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/2209
Affected Version(s): 20h2					
Improper Privilege Management	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22026	O-MIC-WIND-210722/2210
Improper Control of Generation	12-Jul-2022	8.1	Windows Network File System Remote Code Execution	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210722/2211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			Vulnerability. This CVE ID is unique from CVE-2022-22039. **CVE ID : CVE-2022-22029**	US/security-guidance/advisory/CVE-2022-22029	
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22038	O-MIC-WIND-210722/2212
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/2213
Improper Privilege Management	12-Jul-2022	7.8	Windows Credential Guard Domain-joined Public Key Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22031	O-MIC-WIND-210722/2214
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/2215
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22043	O-MIC-WIND-210722/2216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jul-2022	7.8	Windows.Devices.Picker.dll Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22045	O-MIC-WIND-210722/2217
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/2218
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/2219
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.5	Windows Network File System Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22029. **CVE ID : CVE-2022-22039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22039	O-MIC-WIND-210722/2220
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/2221
Improper Privilege	12-Jul-2022	7.2	Windows Print Spooler Elevation of	https://portal.msrc.microsoft	O-MIC-WIND-210722/2222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Privilege Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22041**	.com/en-US/security-guidance/advisory/CVE-2022-22041	
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036	O-MIC-WIND-210722/2223
Exposure of Resource to Wrong Sphere	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30223. **CVE ID : CVE-2022-22042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042	O-MIC-WIND-210722/2224
Exposure of Resource to Wrong Sphere	12-Jul-2022	5.9	Windows Network File System Information Disclosure Vulnerability. **CVE ID : CVE-2022-22028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22028	O-MIC-WIND-210722/2225
Product: windows_server_2019					
Affected Version(s): -					
Improper Privilege Management	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22026	O-MIC-WIND-210722/2226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Windows Network File System Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22039. **CVE ID : CVE-2022-22029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22029	O-MIC-WIND-210722/2227
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22038	O-MIC-WIND-210722/2228
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027. **CVE ID : CVE-2022-22024**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/2229
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/2230
Improper Privilege Management	12-Jul-2022	7.8	Windows Credential Guard Domain-joined Public Key Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22031	O-MIC-WIND-210722/2231
Improper Privilege	12-Jul-2022	7.8	Windows Graphics Component Elevation	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210722/2232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	US/security-guidance/advisory/CVE-2022-22034	
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22043	O-MIC-WIND-210722/2233
Improper Privilege Management	12-Jul-2022	7.8	Windows.Devices.Picker.dll Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22045	O-MIC-WIND-210722/2234
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/2235
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025	O-MIC-WIND-210722/2236
Improper Privilege Management	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037	O-MIC-WIND-210722/2237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22037		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.5	Windows Network File System Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22029. **CVE ID : CVE-2022-22039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22039	O-MIC-WIND-210722/2238
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/2239
Improper Privilege Management	12-Jul-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22041	O-MIC-WIND-210722/2240
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22022	O-MIC-WIND-210722/2241
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-210722/2242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-22036**	guidance/advisory/CVE-2022-22036	
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023	O-MIC-WIND-210722/2243
Exposure of Resource to Wrong Sphere	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30223. **CVE ID : CVE-2022-22042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042	O-MIC-WIND-210722/2244
Exposure of Resource to Wrong Sphere	12-Jul-2022	5.9	Windows Network File System Information Disclosure Vulnerability. **CVE ID : CVE-2022-22028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22028	O-MIC-WIND-210722/2245
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/2246
Product: windows_server_2022					
Affected Version(s): -					
Improper Privilege Management	12-Jul-2022	8.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210722/2247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE-2022-22047, CVE-2022-22049. **CVE ID : CVE-2022-22026**	ory/CVE-2022-22026	
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Windows Network File System Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22039. **CVE ID : CVE-2022-22029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22029	O-MIC-WIND-210722/2248
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22038	O-MIC-WIND-210722/2249
N/A	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22027. **CVE ID : CVE-2022-22024**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024	O-MIC-WIND-210722/2250
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.8	Windows Fax Service Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22024. **CVE ID : CVE-2022-22027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027	O-MIC-WIND-210722/2251
Improper Privilege Management	12-Jul-2022	7.8	Windows Credential Guard Domain-joined Public Key Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210722/2252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22031	ory/CVE-2022-22031	
Improper Privilege Management	12-Jul-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034	O-MIC-WIND-210722/2253
Improper Privilege Management	12-Jul-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22043	O-MIC-WIND-210722/2254
Improper Privilege Management	12-Jul-2022	7.8	Windows.Devices.Picker.dll Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22045	O-MIC-WIND-210722/2255
Improper Privilege Management	12-Jul-2022	7.8	Windows CSRSS Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22026, CVE-2022-22049. **CVE ID : CVE-2022-22047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047	O-MIC-WIND-210722/2256
N/A	12-Jul-2022	7.5	Windows Internet Information Services Cachuri Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025	O-MIC-WIND-210722/2257
Improper Privilege	12-Jul-2022	7.5	Windows Advanced Local Procedure Call Elevation of Privilege	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210722/2258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Vulnerability. This CVE ID is unique from CVE-2022-30202, CVE-2022-30224. **CVE ID : CVE-2022-22037**	US/security-guidance/advisory/CVE-2022-22037	
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	7.5	Windows Network File System Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22029. **CVE ID : CVE-2022-22039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22039	O-MIC-WIND-210722/2259
Uncontrolled Resource Consumption	12-Jul-2022	7.3	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability. **CVE ID : CVE-2022-22040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040	O-MIC-WIND-210722/2260
Improper Privilege Management	12-Jul-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22041	O-MIC-WIND-210722/2261
N/A	12-Jul-2022	7.1	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22041, CVE-2022-30206, CVE-2022-30226. **CVE ID : CVE-2022-22022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22022	O-MIC-WIND-210722/2262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	12-Jul-2022	7	Performance Counters for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036	O-MIC-WIND-210722/2263
N/A	12-Jul-2022	6.6	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-22023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023	O-MIC-WIND-210722/2264
Exposure of Resource to Wrong Sphere	12-Jul-2022	6.5	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30223. **CVE ID : CVE-2022-22042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042	O-MIC-WIND-210722/2265
Exposure of Resource to Wrong Sphere	12-Jul-2022	5.9	Windows Network File System Information Disclosure Vulnerability. **CVE ID : CVE-2022-22028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22028	O-MIC-WIND-210722/2266
Exposure of Resource to Wrong Sphere	12-Jul-2022	4.7	Windows Kernel Information Disclosure Vulnerability. **CVE ID : CVE-2022-21845**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845	O-MIC-WIND-210722/2267
Vendor: Nvidia					
Product: dgx_a100_firmware					
Affected Version(s): * Up to (excluding) 22.5.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jul-2022	8.2	NVIDIA DGX A100 contains a vulnerability in SBIOS in the BiosCfgTool, where a local user with elevated privileges can read and write beyond intended bounds in SMRAM, which may lead to code execution, escalation of privileges, denial of service, and information disclosure. The scope of impact can extend to other components. **CVE ID : CVE-2022-28200**	https://nvidia.custhelp.com/app/answers/detail/a_id/5367	O-NVI-DGX_-210722/2268
Access of Uninitialized Pointer	04-Jul-2022	8.2	NVIDIA DGX A100 contains a vulnerability in SBIOS in the Ofbd, where a local user with elevated privileges can cause access to an uninitialized pointer, which may lead to code execution, escalation of privileges, denial of service, and information disclosure. The scope of impact can extend to other components. **CVE ID : CVE-2022-31599**	https://nvidia.custhelp.com/app/answers/detail/a_id/5367	O-NVI-DGX_-210722/2269
Integer Overflow or	04-Jul-2022	8.2	NVIDIA DGX A100 contains a vulnerability in SBIOS in the SmmCore,	https://nvidia.custhelp.com/app/answers/d	O-NVI-DGX_-210722/2270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			where a user with high privileges can chain another vulnerability to this vulnerability, causing an integer overflow, possibly leading to code execution, escalation of privileges, denial of service, compromised integrity, and information disclosure. The scope of impact can extend to other components. **CVE ID : CVE-2022-31600**	etail/a_id/5367	
Out-of-bounds Write	04-Jul-2022	6.7	NVIDIA DGX A100 contains a vulnerability in SBIOS in the SmbiosPei, which may allow a highly privileged local attacker to cause an out-of-bounds write, which may lead to code execution, denial of service, compromised integrity, and information disclosure. **CVE ID : CVE-2022-31601**	https://nvidia.custhelp.com/app/answers/detail/a_id/5367	O-NVI-DGX_-210722/2271
Out-of-bounds Write	04-Jul-2022	6.7	NVIDIA DGX A100 contains a vulnerability in SBIOS in the IpSecDxe, where a user with elevated privileges and a preconditioned heap can exploit an	https://nvidia.custhelp.com/app/answers/detail/a_id/5367	O-NVI-DGX_-210722/2272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out-of-bounds write vulnerability, which may lead to code execution, denial of service, data integrity impact, and information disclosure. **CVE ID : CVE-2022-31602**		
Improper Validation of Array Index	04-Jul-2022	6.7	NVIDIA DGX A100 contains a vulnerability in SBIOS in the IpSecDxe, where a user with high privileges and preconditioned IpSecDxe global data can exploit improper validation of an array index to cause code execution, which may lead to denial of service, data integrity impact, and information disclosure. **CVE ID : CVE-2022-31603**	https://nvidia.custhelp.com/app/answers/detail/a_id/5367	O-NVI-DGX_-210722/2273
Vendor: Omron					
Product: na5-12w_firmware					
Affected Version(s): * Up to (including) 1.15					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NA5--210722/2274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NA5--210722/2275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Product: na5-15w_firmware					
Affected Version(s): * Up to (including) 1.15					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NA5--210722/2276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NA5--210722/2277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Product: na5-7w_firmware					
Affected Version(s): * Up to (including) 1.15					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NA5--210722/2278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NA5--210722/2279
Product: na5-9w_firmware					
Affected Version(s): * Up to (including) 1.15					
Authentication	04-Jul-2022	8.1	Authentication bypass by capture-	https://www.ia.omron.com/p	O-OMR-NA5--210722/2280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bypass by Capture-replay			replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	roduct/vulnerability/OMSR-2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NA5--210722/2281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Product: nj-pa3001_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier,	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ-P-210722/2282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ-P-210722/2283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ-P-210722/2284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nj-pd3001_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ-P-210722/2285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ-P-210722/2286
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ-P-210722/2287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj101-1000_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ10-210722/2288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ10-210722/2289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ10-210722/2290
Product: nj101-1020_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ10-210722/2291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier,	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ10-210722/2292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ10-210722/2293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj101-9000_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio'	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ10-210722/2294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ10-210722/2295
Authentication Bypass by	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	O-OMR-NJ10-210722/2296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	2022-002_en.pdf	
Product: nj101-9020_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ10-210722/2297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ10-210722/2298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ10-210722/2299
Product: nj301-1100_firmware					
Affected Version(s): * Up to (including) 1.48					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ30-210722/2300
Authentication Bypass by	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-	O-OMR-NJ30-210722/2301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier,	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ30-210722/2302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj301-1200_firmware					
Affected Version(s): * Up to (excluding) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ30-210722/2303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ30-210722/2304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34151		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ30-210722/2305
Product: nj501-1300_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS)	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj501-1320_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2310
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-	O-OMR-NJ50-210722/2311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	2022-002_en.pdf	
Product: nj501-1340_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2314
Product: nj501-140_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication	04-Jul-2022	8.1	Authentication bypass by capture-	https://www.ia.omron.com/p	O-OMR-NJ50-210722/2315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bypass by Capture-replay			replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	roduct/vulnerability/OMSR-2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj501-1420_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2320
Product: nj501-1500_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nj501-1520_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2325
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj501-4300_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2329
Product: nj501-4310_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	O-OMR-NJ50-210722/2330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj501-4320_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2335
Product: nj501-4400_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nj501-4500_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2340
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj501-5300_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2344
Product: nj501-r300_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	O-OMR-NJ50-210722/2345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj501-r320_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2350
Product: nj501-r400_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nj501-r420_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2355
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nj501-r500_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2359
Product: nj501-r520_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	O-OMR-NJ50-210722/2360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NJ50-210722/2361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NJ50-210722/2362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx102-1000_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX10-210722/2363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX10-210722/2364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX10-210722/2365
Product: nx102-1020_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX10-210722/2366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX10-210722/2367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX10-210722/2368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nx102-1100_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX10-210722/2369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX10-210722/2370
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX10-210722/2371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx102-1120_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX10-210722/2372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX10-210722/2373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX10-210722/2374
Product: nx102-1200_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	O-OMR-NX10-210722/2375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX10-210722/2376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX10-210722/2377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx102-1220_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX10-210722/2378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX10-210722/2379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX10-210722/2380
Product: nx102-9020_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX10-210722/2381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX10-210722/2382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX10-210722/2383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nx1p2-1040dt1_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1P-210722/2384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1P-210722/2385
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX1P-210722/2386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx1p2-1040dt_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1P-210722/2387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1P-210722/2388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX1P-210722/2389
Product: nx1p2-1140dt1_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	O-OMR-NX1P-210722/2390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1P-210722/2391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX1P-210722/2392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx1p2-1140dt_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1P-210722/2393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1P-210722/2394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX1P-210722/2395
Product: nx1p2-9024dt1_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1P-210722/2396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1P-210722/2397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX1P-210722/2398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nx1p2-9024dt_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1P-210722/2399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1P-210722/2400
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX1P-210722/2401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx1w-adb21_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1W-210722/2402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1W-210722/2403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX1W-210722/2404
Product: nx1w-cif01_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	O-OMR-NX1W-210722/2405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1W-210722/2406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX1W-210722/2407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx1w-cif11_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1W-210722/2408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1W-210722/2409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX1W-210722/2410
Product: nx1w-cif12_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1W-210722/2411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1W-210722/2412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX1W-210722/2413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nx1w-dab21v_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1W-210722/2414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1W-210722/2415
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX1W-210722/2416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx1w-mab221_firmware					
Affected Version(s): * Up to (including) 1.48					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1W-210722/2417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX1W-210722/2418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX1W-210722/2419
Product: nx701-1600_firmware					
Affected Version(s): * Up to (including) 1.28					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	O-OMR-NX70-210722/2420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX70-210722/2421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX70-210722/2422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx701-1620_firmware					
Affected Version(s): * Up to (including) 1.28					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX70-210722/2423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX70-210722/2424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX70-210722/2425
Product: nx701-1700_firmware					
Affected Version(s): * Up to (including) 1.28					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX70-210722/2426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX70-210722/2427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX70-210722/2428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33971		
Product: nx701-1720_firmware					
Affected Version(s): * Up to (including) 1.28					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller.	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX70-210722/2429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33208		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX70-210722/2430
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX70-210722/2431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Product: nx701-z600_firmware					
Affected Version(s): * Up to (including) 1.28					
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX70-210722/2432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**		
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX70-210722/2433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX70-210722/2434
Product: nx701-z700_firmware					
Affected Version(s): * Up to (including) 1.28					
Authentication Bypass by	04-Jul-2022	8.1	Authentication bypass by capture-replay vulnerability exists in Machine	https://www.ia.omron.com/product/vulnerability/OMSR-	O-OMR-NX70-210722/2435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			automation controller NJ series all models V 1.48 and earlier, Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who can analyze the communication between the affected controller and automation software 'Sysmac Studio' and/or a Programmable Terminal (PT) to access the controller. **CVE ID : CVE-2022-33208**	2022-001_en.pdf	
Authentication Bypass by Capture-replay	04-Jul-2022	8.1	Use of hard-coded credentials vulnerability exists in Machine automation controller NJ series all models V 1.48 and earlier, Machine automation controller	https://www.ia.omron.com/product/vulnerability/OMSR-2022-001_en.pdf	O-OMR-NX70-210722/2436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, Automation software 'Sysmac Studio' all models V1.49 and earlier, and Programmable Terminal (PT) NA series NA5-15W/NA5-12W/NA5-9W/NA5-7W models Runtime V1.15 and earlier, which may allow a remote attacker who successfully obtained the user credentials by analyzing the affected product to access the controller. **CVE ID : CVE-2022-34151**		
Authentication Bypass by Capture-replay	04-Jul-2022	7.5	Authentication bypass by capture-replay vulnerability exists in Machine automation controller NX7 series all models V1.28 and earlier, Machine automation controller NX1 series all models V1.48 and earlier, and Machine automation controller NJ series all models V 1.48 and earlier, which may allow an adjacent attacker who can analyze the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2022-002_en.pdf	O-OMR-NX70-210722/2437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between the controller and the specific software used by OMRON internally to cause a denial-of-service (DoS) condition or execute a malicious program. **CVE ID : CVE-2022-33971**		
Vendor: Siemens					
Product: scalance_x200-4p_irt_firmware					
Affected Version(s): *					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x201-3p_irt_firmware					
Affected Version(s): *					
Use of Insufficient	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P	https://cert-portal.siemens.com/productce	O-SIE-SCAL-210722/2441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions <		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x201-3p_irt_pro_firmware					
Affected Version(s): *					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	O-SIE-SCAL-210722/2446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26649		
Product: scalance_x202-2irt_firmware					
Affected Version(s): *					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x202-2p_irt_firmware					
Affected Version(s): *					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	O-SIE-SCAL-210722/2451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x202-2p_irt_pro_firmware					
Affected Version(s): *					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x204-2fm_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficient	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	O-SIE-SCAL-210722/2456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6),	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x204-2ld_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26649		
Product: scalance_x204-2ld_ts_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x204-2ts_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	O-SIE-SCAL-210722/2466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x204-2_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x204irt_firmware					
Affected Version(s): *					
Use of Insufficient	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	O-SIE-SCAL-210722/2471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6),	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x204irt_pro_firmware					
Affected Version(s): *					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26649		
Product: scalance_x206-1ld_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x206-1_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	O-SIE-SCAL-210722/2481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x208_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x208_pro_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficient	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	O-SIE-SCAL-210722/2486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6),	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x212-2ld_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26649		
Product: scalance_x212-2_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x216_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	O-SIE-SCAL-210722/2496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_x224_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_xf201-3p_irt_firmware					
Affected Version(s): *					
Use of Insufficient	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	O-SIE-SCAL-210722/2501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6),	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_xf202-2p_irt_firmware					
Affected Version(s): *					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26649		
Product: scalance_xf204-2ba_irt_firmware					
Affected Version(s): *					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_xf204-2_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	O-SIE-SCAL-210722/2511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_xf204irt_firmware					
Affected Version(s): *					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_xf204_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficient	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions),	https://cert-portal.siemens.com/productce	O-SIE-SCAL-210722/2516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions	rt/pdf/ssa-310038.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6),	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: scalance_xf206-1_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26649		
Product: scalance_xf208_firmware					
Affected Version(s): * Up to (excluding) 5.2.6					
Use of Insufficiently Random Values	12-Jul-2022	9.8	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions. **CVE ID : CVE-2022-26647**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions), SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26648**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Jul-2022	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions), SCALANCE X200-4P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X201-3P IRT PRO (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2IRT (All versions), SCALANCE X202-2P IRT (All versions), SCALANCE X202-2P IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-310038.pdf	O-SIE-SCAL-210722/2524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X202-2P IRT PRO (All versions), SCALANCE X204-2 (All versions < V5.2.6), SCALANCE X204-2FM (All versions < V5.2.6), SCALANCE X204-2LD (All versions < V5.2.6), SCALANCE X204-2LD TS (All versions < V5.2.6), SCALANCE X204-2TS (All versions < V5.2.6), SCALANCE X204IRT (All versions), SCALANCE X204IRT (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X204IRT PRO (All versions), SCALANCE X206-1 (All versions < V5.2.6), SCALANCE X206-1LD (All versions < V5.2.6), SCALANCE X208 (All versions < V5.2.6), SCALANCE X208PRO (All versions < V5.2.6), SCALANCE X212-2 (All versions < V5.2.6), SCALANCE X212-2LD (All versions < V5.2.6), SCALANCE X216 (All versions < V5.2.6), SCALANCE X224 (All versions < V5.2.6), SCALANCE XF201-3P IRT (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE XF202-2P IRT (All versions), SCALANCE XF204 (All versions < V5.2.6), SCALANCE XF204-2 (All versions < V5.2.6), SCALANCE XF204-2BA IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF204IRT (All versions), SCALANCE XF206-1 (All versions < V5.2.6), SCALANCE XF208 (All versions < V5.2.6). Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices. **CVE ID : CVE-2022-26649**		
Product: simatic_cp_1242-7_v2_firmware					
Affected Version(s): *					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions),	https://cert-portal.siemens.com/productce	O-SIE-SIMA-210722/2526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**	rt/pdf/ssa-517377.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: simatic_cp_1243-1_firmware					
Affected Version(s): *					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: simatic_cp_1243-7_lte_eu_firmware					
Affected Version(s): *					
Improper Neutralization of Special Elements used in a Command ('Comman	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: simatic_cp_1243-7_lte_us_firmware					
Affected Version(s): *					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0),	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: simatic_cp_1243-8_irc_firmware					
Affected Version(s): *					
Improper Neutralization of Special	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions),	https://cert-portal.siemens.com/productce	O-SIE-SIMA-210722/2537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary	rt/pdf/ssa-517377.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: simatic_cp_1542sp-1_irc_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: simatic_cp_1543-1_firmware					
Affected Version(s): * Up to (excluding) 3.0.22					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: simatic_cp_1543sp-1_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIMA-210722/2548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34819		
Product: simatic_mv540_h_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Insufficient Session Expiration	12-Jul-2022	8	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). The web session management of affected devices does not invalidate session ids in certain logout scenarios. This could allow an authenticated remote attacker to hijack other users' sessions. **CVE ID : CVE-2022-33137**	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	O-SIE-SIMA-210722/2549
Missing Authentication for Critical Function	12-Jul-2022	7.5	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3),	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	O-SIE-SIMA-210722/2550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC MV560 X (All versions < V3.3). Affected devices do not perform authentication for several web API endpoints. This could allow an unauthenticated remote attacker to read and download data from the device. **CVE ID : CVE-2022-33138**		
Product: simatic_mv540_s_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Insufficient Session Expiration	12-Jul-2022	8	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). The web session management of affected devices does not invalidate session ids in certain logout scenarios. This could allow an authenticated remote attacker to hijack other users' sessions. **CVE ID : CVE-2022-33137**	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	O-SIE-SIMA-210722/2551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	12-Jul-2022	7.5	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). Affected devices do not perform authentication for several web API endpoints. This could allow an unauthenticated remote attacker to read and download data from the device. **CVE ID : CVE-2022-33138**	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	O-SIE-SIMA-210722/2552
Product: simatic_mv550_h_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Insufficient Session Expiration	12-Jul-2022	8	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). The web session	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	O-SIE-SIMA-210722/2553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management of affected devices does not invalidate session ids in certain logout scenarios. This could allow an authenticated remote attacker to hijack other users' sessions. **CVE ID : CVE-2022-33137**		
Missing Authentication for Critical Function	12-Jul-2022	7.5	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). Affected devices do not perform authentication for several web API endpoints. This could allow an unauthenticated remote attacker to read and download data from the device. **CVE ID : CVE-2022-33138**	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	O-SIE-SIMA-210722/2554
Product: simatic_mv550_s_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Insufficient Session Expiration	12-Jul-2022	8	A vulnerability has been identified in SIMATIC MV540 H	https://cert-portal.siemens.com/productce	O-SIE-SIMA-210722/2555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). The web session management of affected devices does not invalidate session ids in certain logout scenarios. This could allow an authenticated remote attacker to hijack other users' sessions. **CVE ID : CVE-2022-33137**	rt/pdf/ssa-348662.pdf	
Missing Authentication for Critical Function	12-Jul-2022	7.5	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). Affected devices do not perform authentication for several web API endpoints. This could allow an	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	O-SIE-SIMA-210722/2556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote attacker to read and download data from the device. **CVE ID : CVE-2022-33138**		
Product: simatic_mv560_u_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Insufficient Session Expiration	12-Jul-2022	8	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). The web session management of affected devices does not invalidate session ids in certain logout scenarios. This could allow an authenticated remote attacker to hijack other users' sessions. **CVE ID : CVE-2022-33137**	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	O-SIE-SIMA-210722/2557
Missing Authentication for Critical Function	12-Jul-2022	7.5	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3),	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	O-SIE-SIMA-210722/2558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). Affected devices do not perform authentication for several web API endpoints. This could allow an unauthenticated remote attacker to read and download data from the device. **CVE ID : CVE-2022-33138**		
Product: simatic_mv560_x_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Insufficient Session Expiration	12-Jul-2022	8	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). The web session management of affected devices does not invalidate session ids in certain logout scenarios. This could allow an authenticated remote	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	O-SIE-SIMA-210722/2559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to hijack other users' sessions. **CVE ID : CVE-2022-33137**		
Missing Authentication for Critical Function	12-Jul-2022	7.5	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3), SIMATIC MV540 S (All versions < V3.3), SIMATIC MV550 H (All versions < V3.3), SIMATIC MV550 S (All versions < V3.3), SIMATIC MV560 U (All versions < V3.3), SIMATIC MV560 X (All versions < V3.3). Affected devices do not perform authentication for several web API endpoints. This could allow an unauthenticated remote attacker to read and download data from the device. **CVE ID : CVE-2022-33138**	https://cert-portal.siemens.com/productcert/pdf/ssa-348662.pdf	O-SIE-SIMA-210722/2560
Product: siplus_et_200sp_cp_1542sp-1_irc_tx_rail_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: siplus_et_200sp_cp_1543sp-1_isec_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0),	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: siplus_et_200sp_cp_1543sp-1_isec_tx_rail_firmware					
Affected Version(s): -					
Improper Neutralization of Special	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions),	https://cert-portal.siemens.com/productce	O-SIE-SIPL-210722/2567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary	rt/pdf/ssa-517377.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: siplus_net_cp_1242-7_v2_firmware					
Affected Version(s): *					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: siplus_net_cp_1543-1_firmware					
Affected Version(s): * Up to (excluding) 3.0.22					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Product: siplus_s7-1200_cp_1243-1_firmware					
Affected Version(s): *					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34819		
Product: siplus_s7-1200_cp_1243-1_rail_firmware					
Affected Version(s): *					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application does not	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34820**		
Improper Control of Generation of Code ('Code Injection')	12-Jul-2022	9.8	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges. **CVE ID : CVE-2022-34821**		
Out-of-bounds Write	12-Jul-2022	10	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1542SP-1 IRC (All versions >= V2.0), SIMATIC CP 1543-1 (All versions < V3.0.22), SIMATIC CP 1543SP-1 (All versions >= V2.0), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (All versions >= V2.0), SIPLUS ET 200SP CP 1543SP-1 ISEC (All versions >= V2.0), SIPLUS ET	https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf	O-SIE-SIPL-210722/2581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			200SP CP 1543SP-1 ISEC TX RAIL (All versions >= V2.0), SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET CP 1543-1 (All versions < V3.0.22), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions). The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device. **CVE ID : CVE-2022-34819**		
Vendor: Tenda					
Product: ac10_firmware					
Affected Version(s): 15.03.06.26					
Improper Control of Generation of Code ('Code Injection')	07-Jul-2022	9.8	Tenda AC10 US_AC10V1.0RTL_V15.03.06.26_multi_TD01 was discovered to contain a remote code execution (RCE) vulnerability via the lanIp parameter. **CVE ID : CVE-2022-32054**	https://github.com/winmt/CVE/blob/main/Tenda%20AC10/README.md	O-TEN-AC10-210722/2582
Product: ax1803_firmware					
Affected Version(s): 1.0.0.1_2890					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	9.8	Tenda AX1803 v1.0.0.1_2890 was discovered to contain a command injection vulnerability via the function setipv6status. **CVE ID : CVE-2022-34595**	N/A	O-TEN-AX18-210722/2583
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	9.8	Tenda AX1803 v1.0.0.1_2890 was discovered to contain a command injection vulnerability via the function WanParameterSetting. **CVE ID : CVE-2022-34596**	N/A	O-TEN-AX18-210722/2584
Product: ax1806_firmware					
Affected Version(s): 1.0.0.1					
Out-of-bounds Write	01-Jul-2022	9.8	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the deviceList parameter in the function formAddMacfilterRule. **CVE ID : CVE-2022-32032**	N/A	O-TEN-AX18-210722/2585
Improper Neutralization of Special Elements used in a Command ('Comman	06-Jul-2022	9.8	Tenda AX1806 v1.0.0.1 was discovered to contain a command injection vulnerability via the function WanParameterSetting.	N/A	O-TEN-AX18-210722/2586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			**CVE ID : CVE-2022-34597**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the list parameter in the function formSetQosBand. **CVE ID : CVE-2022-32030**	N/A	O-TEN-AX18-210722/2587
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the list parameter in the function fromSetRouteStatic. **CVE ID : CVE-2022-32031**	N/A	O-TEN-AX18-210722/2588
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow via the function formSetVirtualSer. **CVE ID : CVE-2022-32033**	N/A	O-TEN-AX18-210722/2589
Product: m3_firmware					
Affected Version(s): 1.0.0.12					
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the function formSetAPCfg. **CVE ID : CVE-2022-32037**	N/A	O-TEN-M3_F-210722/2590
Allocation of	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to	N/A	O-TEN-M3_F-210722/2591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resources Without Limits or Throttling			contain a stack overflow via the listN parameter in the function fromDhcpListClient. **CVE ID : CVE-2022-32039**		
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the function formSetCfm. **CVE ID : CVE-2022-32040**	N/A	O-TEN-M3_F-210722/2592
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the function formGetPassengerAnalyseData. **CVE ID : CVE-2022-32041**	N/A	O-TEN-M3_F-210722/2593
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the function formSetAccessCodeInfo. **CVE ID : CVE-2022-32043**	N/A	O-TEN-M3_F-210722/2594
Vendor: Tendacn					
Product: ac23_ac2100_firmware					
Affected Version(s): 16.03.07.44					
Out-of-bounds Write	06-Jul-2022	9.8	Tenda AC23 v16.03.07.44 was discovered to contain a stack overflow via the	N/A	O-TEN-AC23-210722/2595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AdvSetMacMtuWan function. **CVE ID : CVE-2022-32383**		
Out-of-bounds Write	06-Jul-2022	9.8	Tenda AC23 v16.03.07.44 is vulnerable to Stack Overflow that will allow for the execution of arbitrary code (remote). **CVE ID : CVE-2022-32385**	N/A	O-TEN-AC23-210722/2596
Out-of-bounds Write	06-Jul-2022	9.8	Tenda AC23 v16.03.07.44 was discovered to contain a buffer overflow via fromAdvSetMacMtuWan. **CVE ID : CVE-2022-32386**	N/A	O-TEN-AC23-210722/2597
Out-of-bounds Write	01-Jul-2022	8.8	Tenda AC23 v16.03.07.44 was discovered to contain a stack overflow via the security_5g parameter in the function formWifiBasicSet. **CVE ID : CVE-2022-32384**	N/A	O-TEN-AC23-210722/2598
Product: m3_firmware					
Affected Version(s): 1.0.0.12					
Improper Restriction of Operations within the Bounds of	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the items parameter in the function formdelMasteraclist.	N/A	O-TEN-M3_F-210722/2599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			**CVE ID : CVE-2022-32034**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to contain a stack overflow via the function formMasterMng. **CVE ID : CVE-2022-32035**	N/A	O-TEN-M3_F-210722/2600
Out-of-bounds Write	01-Jul-2022	7.5	Tenda M3 V1.0.0.12 was discovered to contain multiple stack overflow vulnerabilities via the ssidList, storeName, and trademark parameters in the function formSetStoreWeb. **CVE ID : CVE-2022-32036**	N/A	O-TEN-M3_F-210722/2601
Vendor: totolink					
Product: a3000ru_firmware					
Affected Version(s): 5.9c.5185_b20201128					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	7.2	Totolink A830R V5.9c.4729_B20191112, Totolink A3100R V4.1.2cu.5050_B20200504, Totolink A950RG V4.1.2cu.5161_B20200903, Totolink A800R V4.1.2cu.5137_B20200730, Totolink A3000RU V5.9c.5185_B20201128, Totolink A810R V4.1.2cu.5182_B20201026 were discovered to contain	N/A	O-TOT-A300-210722/2602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a command injection vulnerability. **CVE ID : CVE-2022-28935**		
Product: a3100r_firmware					
Affected Version(s): 4.1.2cu.5050_b20200504					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	7.2	Totolink A830R V5.9c.4729_B20191112, Totolink A3100R V4.1.2cu.5050_B20200504, Totolink A950RG V4.1.2cu.5161_B20200903, Totolink A800R V4.1.2cu.5137_B20200730, Totolink A3000RU V5.9c.5185_B20201128, Totolink A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability. **CVE ID : CVE-2022-28935**	N/A	O-TOT-A310-210722/2603
Product: a800r_firmware					
Affected Version(s): 4.1.2cu.5137_b20200730					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	7.2	Totolink A830R V5.9c.4729_B20191112, Totolink A3100R V4.1.2cu.5050_B20200504, Totolink A950RG V4.1.2cu.5161_B20200903, Totolink A800R V4.1.2cu.5137_B20200730, Totolink A3000RU V5.9c.5185_B20201128, Totolink A810R	N/A	O-TOT-A800-210722/2604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability. **CVE ID : CVE-2022-28935**		
Product: a810r_firmware					
Affected Version(s): 4.1.2cu.5182_b20201026					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	7.2	Totolink A830R V5.9c.4729_B20191112, Totolink A3100R V4.1.2cu.5050_B20200504, Totolink A950RG V4.1.2cu.5161_B20200903, Totolink A800R V4.1.2cu.5137_B20200730, Totolink A3000RU V5.9c.5185_B20201128, Totolink A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability. **CVE ID : CVE-2022-28935**	N/A	O-TOT-A810-210722/2605
Product: a830r_firmware					
Affected Version(s): 5.9c.4729_b20191112					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	7.2	Totolink A830R V5.9c.4729_B20191112, Totolink A3100R V4.1.2cu.5050_B20200504, Totolink A950RG V4.1.2cu.5161_B20200903, Totolink A800R V4.1.2cu.5137_B20200730, Totolink	N/A	O-TOT-A830-210722/2606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A3000RU V5.9c.5185_B20201128, Totolink A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability. **CVE ID : CVE-2022-28935**		
Product: a950rg_firmware					
Affected Version(s): 4.1.2cu.5161_b20200903					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2022	7.2	Totolink A830R V5.9c.4729_B20191112, Totolink A3100R V4.1.2cu.5050_B20200504, Totolink A950RG V4.1.2cu.5161_B20200903, Totolink A800R V4.1.2cu.5137_B20200730, Totolink A3000RU V5.9c.5185_B20201128, Totolink A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability. **CVE ID : CVE-2022-28935**	N/A	O-TOT-A950-210722/2607
Product: ex300_v2_firmware					
Affected Version(s): 4.0.3c.7484					
Improper Neutralization of Special Elements used in a Command	07-Jul-2022	9.8	TOTOLINK EX300_V2 V4.0.3c.7484 was discovered to contain a command injection vulnerability via the langType parameter in the setLanguageCfg	N/A	O-TOT-EX30-210722/2608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			function. This vulnerability is exploitable via a crafted MQTT data packet. **CVE ID : CVE-2022-32449**		
Product: t6_firmware					
Affected Version(s): 4.1.9cu.5179_b20201015					
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the password parameter in the function FUN_00413f80. **CVE ID : CVE-2022-32044**	https://github.com/d1tto/IoT-vuln/tree/main/Totolink/T6-v2/5.setWiFiRepeaterCfg	O-TOT-T6_F-210722/2609
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the desc parameter in the function FUN_00413be4. **CVE ID : CVE-2022-32045**	N/A	O-TOT-T6_F-210722/2610
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the desc parameter in the function FUN_0041880c. **CVE ID : CVE-2022-32046**	N/A	O-TOT-T6_F-210722/2611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the desc parameter in the function FUN_00412ef4. **CVE ID : CVE-2022-32047**	N/A	O-TOT-T6_F-210722/2612
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the command parameter in the function FUN_0041cc88. **CVE ID : CVE-2022-32048**	N/A	O-TOT-T6_F-210722/2613
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the url parameter in the function FUN_00418540. **CVE ID : CVE-2022-32049**	N/A	O-TOT-T6_F-210722/2614
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the cloneMac parameter in the function FUN_0041af40. **CVE ID : CVE-2022-32050**	N/A	O-TOT-T6_F-210722/2615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the desc, week, sTime, eTime parameters in the function FUN_004133c4. **CVE ID : CVE-2022-32051**	N/A	O-TOT-T6_F-210722/2616
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the desc parameter in the function FUN_004137a4. **CVE ID : CVE-2022-32052**	N/A	O-TOT-T6_F-210722/2617
Allocation of Resources Without Limits or Throttling	01-Jul-2022	7.5	TOTOLINK T6 V4.1.9cu.5179_B20201015 was discovered to contain a stack overflow via the cloneMac parameter in the function FUN_0041621c. **CVE ID : CVE-2022-32053**	N/A	O-TOT-T6_F-210722/2618
Vendor: wavlink					
Product: wl-wn575a3_firmware					
Affected Version(s): rpt75a3.v4300.201217					
Improper Neutralization of Special Elements used in a Command	07-Jul-2022	9.8	Wavlink WL-WN575A3 RPT75A3.V4300.201217 was discovered to contain a command injection vulnerability via the function obtw.	N/A	O-WAV-WL-W-210722/2619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			This vulnerability allows attackers to execute arbitrary commands via a crafted POST request. **CVE ID : CVE-2022-34592**		
Vendor: webhmi					
Product: webhmi_firmware					
Affected Version(s): * Up to (including) 4.1.1.7662					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2022	9.1	A user with administrative privileges in Distributed Data Systems WebHMI 4.1.1.7662 may send OS commands to execute on the host server. **CVE ID : CVE-2022-2253**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-181-04	O-WEB-WEBH-210722/2620
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jul-2022	4.8	A user with administrative privileges in Distributed Data Systems WebHMI 4.1.1.7662 can store a script that could impact other logged in users. **CVE ID : CVE-2022-2254**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-181-04	O-WEB-WEBH-210722/2621
Vendor: XEN					
Product: xen					
Affected Version(s): -					
N/A	05-Jul-2022	7.8	network backend may cause Linux netfront to use freed SKBs While adding logic to support XDP (eXpress	https://xenbits.xenproject.org/xsa/advisory-405.txt, http://xenbits.	O-XEN-XEN-210722/2622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Data Path), a code label was moved in a way allowing for SKBs having references (pointers) retained for further processing to nevertheless be freed. **CVE ID : CVE-2022-33743**	xen.org/xsa/advisory-405.html, http://www.openwall.com/lists/oss-security/2022/07/05/5	
Exposure of Sensitive Information to an Unauthorized Actor	05-Jul-2022	7.1	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742). **CVE ID : CVE-2022-26365**	https://xenbits.xenproject.org/xsa/advisory-403.txt, http://xenbits.xen.org/xsa/advisory-403.html, http://www.openwall.com/lists/oss-security/2022/07/05/6	O-XEN-XEN-210722/2623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	05-Jul-2022	7.1	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742). **CVE ID : CVE-2022-33740**	https://xenbits.xenproject.org/xsa/advisory-403.txt, http://xenbits.xen.org/xsa/advisory-403.html, http://www.openwall.com/lists/oss-security/2022/07/05/6	O-XEN-XEN-210722/2624
Exposure of Sensitive Information to an Unauthorized Actor	05-Jul-2022	7.1	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and	https://xenbits.xenproject.org/xsa/advisory-403.txt, http://xenbits.xen.org/xsa/advisory-403.html, http://www.openwall.com/li	O-XEN-XEN-210722/2625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742). **CVE ID : CVE-2022-33741**	sts/oss-security/2022/07/05/6	
Exposure of Sensitive Information to an Unauthorized Actor	05-Jul-2022	7.1	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't	https://xenbits.xenproject.org/xsa/advisory-403.txt, http://xenbits.xen.org/xsa/advisory-403.html, http://www.openwall.com/lists/oss-security/2022/07/05/6	O-XEN-XEN-210722/2626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742). **CVE ID : CVE-2022-33742**		
Vendor: Yokogawa					
Product: aw810d_firmware					
Affected Version(s): * Up to (including) r12					
Use of Insufficiently Random Values	04-Jul-2022	7.5	Use of insufficiently random values vulnerability exists in Vnet/IP communication module VI461 of YOKOGAWA Wide Area Communication Router (WAC Router) AW810D, which may allow a remote attacker to cause denial-of-service (DoS) condition by sending a specially crafted packet. **CVE ID : CVE-2022-32284**	https://web-material3.yokogawa.com/19/32825/files/YSAR-22-0005-J.pdf, https://web-material3.yokogawa.com/1/32825/files/YSAR-22-0005-E.pdf	O-YOK-AW81-210722/2627