National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

https://nciipc.gov.in/

01 - 15 Apr 2022 Vol. 09 No. 07

Table of Content

Vendor	Product	Page Number
Application		
ad_inserter_project	ad_inserter	1
aenrich	a\+hrd	1
aerocms_project	aerocms	2
allmediaserver	allmediaserver	3
Altn	securitygateway	3
Apache	hadoop	3
	nifi	4
	pinot	5
apusthemes	careerup	6
asana	desktop	6
asciidoctor-include-ext_project	asciidoctor-include-ext	6
atlasgondal	export_all_urls	7
autolabproject	autolab	8
baigo	baigo_cms	8
Barco	control_room_management_suite	8
bettinivideo	sgsetup	9
Bigantsoft	bigant_server	9
Bitdefender	endpoint_security_tools	9
	gravityzone	10
	update_server	11
brew	mruby	12
buildah_project	buildah	12
Busybox	busybox	13
calibre-web_project	calibre-web	13
car_rental_system_project	car_rental_system	15
Cisco	cx_cloud_agent	15
	identity_services_engine	16

Vendor	Product	Page Number
Cisco	secure_network_analytics	18
	telepresence_video_communication_server	18
	ultra_cloud_core	20
	ultra_cloud_core_-_subscriber_microservices_infrastructure	20
	webex_meetings_online	21
	web_security_appliance	22
cocoapods	cocoapods-downloader	23
Codesys	control_for_beaglebone_sl	24
	control_for_beckhoff_cx9020	24
	control_for_empc-a\/imx6_sl	25
	control_for_iot2000_sl	25
	control_for_linux_sl	25
	control_for_pfc100_sl	25
	control_for_pfc200_sl	26
	control_for_plcnext_sl	26
	control_for_raspberry_pi_sl	26
	control_for_wago_touch_panels_600_sl	27
	control_rte_sl	27
	control_rte_sl_\(for_beckhoff_cx\)	27
	control_runtime_system_toolkit	27
	control_win_sl	28
	development_system	28
	edge_gateway	28
	embedded_target_visu_toolkit	29
	gateway	29
	hmi_sl	29
	remote_target_visu_toolkit	30
college_website_content_management_system_project	college_website_content_management_system	30
cozmoslabs	profile_builder	30

Vendor	Product	Page Number
Craftcms	craft_cms	31
crun_project	crun	31
Cybernetikz	easy_social_icons	32
dascomsoft	eziosuite	32
deepmerge-ts_project	deepmerge-ts	33
Dell	alienware_update	33
	command_update	34
	update	34
	wyse_device_agent	34
	wyse_management_suite	36
deltaww	diaenergie	36
dompdf_project	dompdf	36
ecommerce-website_product	ecommerce-website	37
ecommerce-website_project	ecommerce-website	37
elbtide	advanced_booking_calendar	38
employee_performance_evaluation_project	employee_performance_evaluation	39
eyecix	careerfy	39
	jobsearch_wp_job_board	39
febs-security_project	febs-security	40
finn	podium_layout	40
	podium_proxy	41
Foliovision	fv_flowplayer_video_player	42
forcepoint	one_endpoint	43
formbuilder_project	formbuilder	44
Fortinet	fortiedr	45
Fujitsu	plugfree_network	46
fullpage_project	fullpage	46
getbootstrap	bootstrap	46
gimmal	sherpa_connector_service	47
Github	enterprise_server	47
Gitlab	gitlab	48
gnuboard	gnuboard5	55

Vendor	Product	Page Number
Google	chrome	56
gpac	gpac	70
halo	halo	71
HP	oneview	71
htmldoc_project	htmldoc	72
IBM	app_connect_enterprise_certified_container	73
	partner_engagement_manager	73
	planning_analytics	74
	urbancode_deploy	74
	watson_query	75
icehrm	icehrm	75
idearespa	reftree	76
Impresscms	impresscms	76
insights_from_google_pagespeed_project	insights_from_google_pagespeed	77
insurance_management_system_project	insurance_management_system	77
ivanti	dsm_remote	78
	incapptic_connect	78
jellycms	jellycms	78
Jetbrains	ktor	79
jflyfox	jfinal_cms	79
Kaspersky	anti-virus	79
	endpoint_security	80
	internet_security	80
	security_cloud	81
	small_office_security	81
	total_security	81
kopano	groupware_core	82
Kyocera	net_viewer	82
libsixel_project	libsixel	83
Libtiff	libtiff	83

Vendor	Product	Page Number
Linux	linux_kernel	84
livehelperchat	live_helper_chat	84
LUA	lua	86
mappresspro	mappress_maps	86
mark_posts_project	mark_posts	87
material_design_for_contact_form_7_project	material_design_for_contact_form_7	87
matrimony_project	matrimony	88
Microsoft	edge_chromium	88
mingsoft	mcms	91
miraheze	createwiki	91
modbustools	modbus_slave	92
moguit	mogu_blog_cms	92
momentjs	moment	92
movie_seat_reservation_project	movie_seat_reservation	93
mruby	mruby	93
musical_world_project	musical_world	94
Netflix	consoleme	95
newbee-mall_project	newbee-mall	95
nginxproxymanager	nginx_proxy_manager	95
nootheme	jobmonster	95
nsthemes	ns_watermark_for_woocommerce	96
ocdi	one_click_demo_import	97
ofcms_project	ofcms	97
Omron	cx-position	98
online_banking_system_project	online_banking_system	99
online_car_rental_system_project	online_car_rental_system	100
online_project_time_management_system_project	online_project_time_management_system	100
online_sports_complex_booking_project	online_sports_complex_booking	100
online_student_admission_project	online_student_admission	100

Vendor	Product	Page Number
onlyoffice	document_server	101
Orangehrm	orangehrm	101
os4ed	opensis	102
Owncloud	owncloud	102
payroll_management_system_project	payroll_management_system	103
php-cms_project	php-cms	103
Phpipam	phpipam	103
pickplugins	post_grid	104
Pimcore	pimcore	105
pivotal_software	spring_framework	105
pjsip	pjsip	106
plugin-planet	blackhole_for_bad_bots	107
podman_project	podman	108
pootlepress	easy_smooth_scroll_links	108
presscustomizr	nimble_page_builder	109
program	parking_lot_management_system	109
public_knowledge_project	open_journal_systems	110
Qdpm	qdpm	110
Radare	radare2	110
rangerstudio	directus	114
rc-httpd_project	rc-httpd	115
realfavicongenerator	favicon_by_realfavicongenerator	115
Redhat	openshift_container_platform	115
reprisesoftware	reprise_license_manager	117
rocket.chat	livechat	118
Rockwellautomation	connected_components_workbench	118
	isagraf	118
saasproject	booking_package	119
salonbookingsystem	salon_booking_system	119
sap_information_system_project	sap_information_system	120
scala-js	scala.js	121

Vendor	Product	Page Number
school_club_application_system_project	school_club_application_system	121
secom	dr.id_access_control	123
	dr.id_attendance_system	123
secondlinethemes	podcast_importer_secondline	123
simple-git_project	simple-git	124
Simplemachines	simple_machines_forum	124
simple_bakery_shop_management_system_project	simple_bakery_shop_management_system	125
simple_house_rental_system_project	simple_house_rental_system	125
simple_student_information_system_project	simple_student_information_system	125
socialcodia	social_codia_sms	126
std42	elfinder	126
stopbadbots	block_and_stop_bad_bots	127
struktur	libde265	127
student_grading_system_project	student_grading_system	128
Suse	rancher_desktop	128
swayvm	swaylock	128
Synametrics	synaman	129
tableexport.jquery.plugin_project	tableexport.jquery.plugin	129
tastyigniter	tastyigniter	130
thedaylightstudio	fuel_cms	130
thimpress	learnpress	130
tildearrow	furnace	131
tms-outsource	amelia	131
	wpdatatables_lite	132
totaljs	content_management_system	133
tpcms_project	tpcms	133
Trendmicro	antivirus_for_mac	134
trudesk_project	trudesk	134
twistedmatrix	twisted	134

Vendor	Product	Page Number
updraftplus	updraftplus	136
uri.js_project	uri.js	136
url.js_project	url.js	137
vcs_project	vcs	137
vertistudio	image_optimization_\&_lazy_load_by_optimole	137
Vmware	spring_cloud_function	138
	spring_framework	138
vyper_project	vyper	139
waycrate	swhkd	140
webence	iq_block_country	140
Weechat	weechat	141
weseek	growi	142
wisc	htcondor	142
wpdownloadmanager	wordpress_download_manager	143
wpjos	library_file_manager	143
wpvivid	migration\,_backup\,_staging	144
wwbn	avideo	144
wztechno	wyzi	145
Xwiki	Xwiki	145
Yourls	Yourls	146
zbzcms	zbzcms	147
Zohocorp	manageengine_adaudit_plus	148
	manageengine_adselfservice_plus	149
	manageengine_servicedesk_plus	149
	manageengine_supportcenter_plus	149
zoo_management_system_project	zoo_management_system	150
Zyxel	zyxel_ap_configurator	150
Hardware		
Asus	rt-ac86u	151
	rt-ax56u	152
Cisco	asr_5500	154
	asr_5700	154

Vendor	Product	Page Number
Cisco	email_security_appliance	155
	ip_phone_6825	156
	ip_phone_6841	157
	ip_phone_6851	158
	ip_phone_6861	159
	ip_phone_6871	160
	ip_phone_7811	161
	ip_phone_7821	161
	ip_phone_7832	162
	ip_phone_7841	163
	ip_phone_7861	164
	ip_phone_8811	165
	ip_phone_8832	166
	ip_phone_8841	167
	ip_phone_8845	168
	ip_phone_8851	169
	ip_phone_8861	170
	ip_phone_8865	171
	secure_email_and_web_manager	172
	web_security_appliance	173
Digi	passport	175
Dlink	dir-878	176
fantec	mwid25-ds	176
flexwatch	fw3170-ps-e	177
hitrontech	chita	177
mediatek	mt6580	177
	mt6735	178
	mt6737	178
	mt6739	178
	mt6750	179
	mt6753	179
	mt6755	180

Vendor	Product	Page Number
mediatek	mt6762	180
	mt6763	180
	mt6765	181
	mt6768	182
	mt6769	183
	mt6771	184
	mt6779	184
	mt6781	185
	mt6785	186
	mt6789	187
	mt6833	188
	mt6853	189
	mt6853t	190
	mt6873	191
	mt6875	192
	mt6877	192
	mt6879	193
	mt6883	194
	mt6885	195
	mt6889	196
	mt6890	196
	mt6891	197
	mt6893	198
	mt6895	199
	mt6983	199
	mt6985	200
	mt8163	200
	mt8167	201
	mt8167s	202
	mt8168	202
	mt8173	203
	mt8175	204

Vendor	Product	Page Number
mediatek	mt8183	205
	mt8185	205
	mt8321	206
	mt8362a	207
	mt8365	208
	mt8385	209
	mt8666	210
	mt8667	211
	mt8675	213
	mt8735a	213
	mt8735b	214
	mt8765	215
	mt8766	216
	mt8768	218
	mt8786	219
	mt8788	220
	mt8789	222
	mt8791	223
	mt8797	223
Mitsubishielectric	fx5uc	224
	fx5uc-32mr\/ds-ts	227
	fx5uc-32mt\/d	230
	fx5uc-32mt\/ds-ts	233
	fx5uc-32mt\/dss	236
	fx5uc-32mt\/dss-ts	239
	fx5uj	242
	fx5uj-24mr\/es	245
	fx5uj-24mt\/es	248
	fx5uj-24mt\/ess	250
	fx5uj-40mr\/es	253
	fx5uj-40mt\/es	256
	fx5uj-40mt\/ess	259

Vendor	Product	Page Number
Mitsubishielectric	fx5uj-60mr\/es	262
	fx5uj-60mt\/es	265
	fx5uj-60mt\/ess	268
Philips	e-alert	271
Rockwellautomation	compactlogix_5380	271
	compactlogix_5480	272
	compact_guardlogix_5380	272
	controllogix_5580	272
	guardlogix_5580	273
roku	express	273
	express_4k\+	273
	roku_tv	274
	streambar	274
	streambar_pro	274
	streaming_stick_4k	274
	streaming_stick_4k\+	275
	ultra	275
	wireless_speakers	275
	wireless_subwoofer	275
Samsung	t5	276
Tenda	ac9	276
ui	ua_lite	277
Verizon	lvskihp	277
wavlink	wl-wn531p3	278
Xerox	colorqube_8580	278
Zyxel	ax7501-b0	279
	dx5401-b0	279
	emg3525-t50b	280
	emg5523-t50b	281
	emg5723-t50k	281
	emg6726-b10a	282
	ep240p	283

Vendor	Product	Page Number
Zyxel	ex3510-b0	284
	ex5401-b0	284
	ex5501-b0	285
	pm7300-t0	286
	pmg5317-t20b	287
	pmg5617-t20b2	287
	pmg5617ga	288
	pmg5622ga	289
	px7501-b0	290
	vmg1312-t20b	290
	vmg3312-t20a	291
	vmg3625-t50b	292
	vmg3927-b50a	293
	vmg3927-b50b	293
	vmg3927-b60a	294
	vmg3927-t50k	295
	vmg4927-b50a	296
	vmg8623-t50b	296
	vmg8825-b50a	297
	vmg8825-b50b	298
	vmg8825-b60a	299
	vmg8825-b60b	299
	vmg8825-t50k	300
	xmg3927-b50a	301
	xmg8825-b50a	302
Operating System		
Asus	rt-ac86u_firmware	303
	rt-ax56u_firmware	304
Cisco	asyncos	305
	ip_phone_6825_firmware	307
	ip_phone_6841_firmware	308
	ip_phone_6851_firmware	309

Vendor	Product	Page Number
Cisco	ip_phone_6861_firmware	310
	ip_phone_6871_firmware	311
	ip_phone_7811_firmware	312
	ip_phone_7821_firmware	313
	ip_phone_7832_firmware	313
	ip_phone_7841_firmware	314
	ip_phone_7861_firmware	315
	ip_phone_8811_firmware	316
	ip_phone_8832_firmware	317
	ip_phone_8841_firmware	318
	ip_phone_8845_firmware	319
	ip_phone_8851_firmware	320
	ip_phone_8861_firmware	321
	ip_phone_8865_firmware	322
	staros	323
Dell	emc_powerscale_onefs	324
Digi	passport_firmware	326
Dlink	dir-878_firmware	326
fantec	mwid25-ds_firmware	327
Fedoraproject	fedora	327
flexwatch	fw3170-ps-e_firmware	329
Google	android	329
	chrome_os	331
hitrontech	chita_firmware	332
Linux	linux_kernel	332
Microsoft	windows	334
Mitsubishielectric	fx5uc-32mr\/ds-ts_firmware	335
	fx5uc-32mt\/ds-ts_firmware	338
	fx5uc-32mt\/dss-ts_firmware	341
	fx5uc-32mt\/dss_firmware	344
	fx5uc-32mt\/d_firmware	347
	fx5uc_firmware	350

Vendor	Product	Page Number
Mitsubishielectric	fx5uj-24mr\/es_firmware	353
	fx5uj-24mt\/ess_firmware	356
	fx5uj-24mt\/es_firmware	359
	fx5uj-40mr\/es_firmware	362
	fx5uj-40mt\/ess_firmware	365
	fx5uj-40mt\/es_firmware	367
	fx5uj-60mr\/es_firmware	370
	fx5uj-60mt\/ess_firmware	373
	fx5uj-60mt\/es_firmware	376
	fx5uj_firmware	379
Philips	e-alert_firmware	382
Redhat	enterprise_linux	382
Rockwellautomation	compactlogix_5380_firmware	384
	compactlogix_5480_firmware	385
	compact_guardlogix_5380_firmware	385
	controllogix_5580_firmware	386
	guardlogix_5580_firmware	386
	safety_instrumented_systems_workstation	386
roku	roku_os	387
Samsung	t5_firmware	387
Tenda	ac9_firmware	388
ui	ua_lite_firmware	388
Verizon	lvskihp_firmware	389
wavlink	wl-wn531p3_firmware	389
XEN	xen	390
Xerox	colorqube_8580_firmware	395
Zyxel	ax7501-b0_firmware	396
	dx5401-b0_firmware	396
	emg3525-t50b_firmware	397
	emg5523-t50b_firmware	398
	emg5723-t50k_firmware	398
	emg6726-b10a_firmware	399

Vendor	Product	Page Number
Zyxel	ep240p_firmware	400
	ex3510-b0_firmware	401
	ex5401-b0_firmware	401
	ex5501-b0_firmware	402
	pm7300-t0_firmware	403
	pmg5317-t20b_firmware	404
	pmg5617-t20b2_firmware	404
	pmg5617ga_firmware	405
	pmg5622ga_firmware	406
	px7501-b0_firmware	407
	vmg1312-t20b_firmware	407
	vmg3312-t20a_firmware	408
	vmg3625-t50b_firmware	409
	vmg3927-b50a_firmware	410
	vmg3927-b50b_firmware	410
	vmg3927-b60a_firmware	411
	vmg3927-t50k_firmware	412
	vmg4927-b50a_firmware	413
	vmg8623-t50b_firmware	413
	vmg8825-b50a_firmware	414
	vmg8825-b50b_firmware	415
	vmg8825-b60a_firmware	416
	vmg8825-b60b_firmware	416
	vmg8825-t50k_firmware	417
	xmg3927-b50a_firmware	418
	xmg8825-b50a_firmware	419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: ad_inserter_project					
Product: ad_inserter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	6.1	The Ad Inserter Free and Pro WordPress plugins before 2.7.12 do not sanitise and escape the REQUEST_URI before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting in browsers which do not encode characters **CVE ID : CVE-2022-0901**	N/A	A-AD_-AD_I-190422/1
Vendor: aenrich					
Product: a\+hrd					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Apr-22	7.5	aEnrich a+HRD has inadequate filtering for special characters in URLs. An unauthenticated remote attacker can bypass authentication and perform path traversal attacks to access arbitrary files under website root directory. **CVE ID : CVE-2022-26675**	N/A	A-AEN-A\+H-190422/2
Incorrect Authorization	07-Apr-22	9.8	aEnrich a+HRD has inadequate privilege restrictions, an unauthenticated remote attacker can use the API function	N/A	A-AEN-A\+H-190422/3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to upload and execute malicious scripts to control the system or disrupt service. **CVE ID : CVE-2022-26676**		
Vendor: aerocms_project					
Product: aerocms					
Unrestricted Upload of File with Dangerous Type	08-Apr-22	7.2	AeroCMS v0.0.1 was discovered to contain an arbitrary file upload vulnerability via the Post Image function under the Admin panel. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-27061**	N/A	A-AER-AERO-190422/4
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Apr-22	4.8	AeroCMS v0.0.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability via add_post.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Post Title text field. **CVE ID : CVE-2022-27062**	N/A	A-AER-AERO-190422/5
Improper Neutralization of Input During	08-Apr-22	6.1	AeroCMS v0.0.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability via	N/A	A-AER-AERO-190422/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			view_all_comments.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Comments text field. **CVE ID : CVE-2022-27063**		
Vendor: allmediaserver					
Product: allmediaserver					
Out-of-bounds Write	03-Apr-22	9.8	Mediaserver.exe in ALLMediaServer 1.6 has a stack-based buffer overflow that allows remote attackers to execute arbitrary code via a long string to TCP port 888, a related issue to CVE-2017-17932. **CVE ID : CVE-2022-28381**	N/A	A-ALL-ALLM-190422/7
Vendor: Altn					
Product: securitygateway					
XML Injection (aka Blind XPath Injection)	05-Apr-22	5.3	Alt-N MDaemon Security Gateway through 8.5.0 allows SecurityGateway.dll?view=login XML Injection. **CVE ID : CVE-2022-25356**	https://www.swascan.com/security-advisory-alt-n-security-gateway/	A-ALT-SECU-190422/8
Vendor: Apache					
Product: hadoop					
Improper Limitation of a	07-Apr-22	9.8	In Apache Hadoop, The unTar function uses unTarUsingJava	https://lists.apache.org/thread/hslo7wzw24	A-APA-HADO-190422/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			function on Windows and the built-in tar utility on Unix and other OSes. As a result, a TAR entry may create a symlink under the expected extraction directory which points to an external directory. A subsequent TAR entry may extract an arbitrary file into the external directory using the symlink name. This however would be caught by the same targetDirPath check on Unix because of the getCanonicalPath call. However on Windows, getCanonicalPath doesn't resolve symbolic links, which bypasses the check. unpackEntries during TAR extraction follows symbolic links which allows writing outside expected base directory on Windows. This was addressed in Apache Hadoop 3.2.3 **CVE ID : CVE-2022-26612**	49gv1jyjk8g6ttd7935fyz	
Product: nifi					
Insufficiently Protected Credentials	06-Apr-22	4.3	When creating or updating credentials for single-user access, Apache NiFi wrote a	https://nifi.apache.org/security.html#CVE-2022-26850	A-APA-NIFI-190422/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			copy of the Login Identity Providers configuration to the operating system temporary directory. On most platforms, the operating system temporary directory has global read permissions. NiFi immediately moved the temporary file to the final configuration directory, which significantly limited the window of opportunity for access. NiFi 1.16.0 includes updates to replace the Login Identity Providers configuration without writing a file to the operating system temporary directory. **CVE ID : CVE-2022-26850**		
Product: pinot					
Uncontrolled Recursion	05-Apr-22	7.5	In 0.9.3 or older versions of Apache Pinot segment upload path allowed segment directories to be imported into pinot tables. In pinot installations that allow open access to the controller a specially crafted request can potentially be exploited to cause disruption in pinot	https://lists.apache.org/thread/3dk8pf1n02p8oj2j3czbtchyjsf8khwr	A-APA-PINO-190422/11

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service. Pinot release 0.10.0 fixes this. See https://docs.pinot.apache.org/basics/releases/0.10.0 **CVE ID : CVE-2022-23974**		
Vendor: apusthemes					
Product: careerup					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	6.1	There are unauthenticated reflected Cross-Site Scripting (XSS) vulnerabilities in CareerUp Careerup WordPress theme before 2.3.1, via the filter parameters. **CVE ID : CVE-2022-1167**	N/A	A-APU-CARE-190422/12
Vendor: asana					
Product: desktop					
Files or Directories Accessible to External Parties	09-Apr-22	6.5	Asana Desktop before 1.6.0 allows remote attackers to exfiltrate local files if they can trick the Asana desktop app into loading a malicious web page. **CVE ID : CVE-2022-26877**	https://forum.asana.com/t/asana-desktop-app-security-update/160477	A-ASA-DESK-190422/13
Vendor: asciidoctor-include-ext_project					
Product: asciidoctor-include-ext					
Improper Neutralization of Special Elements used in an	01-Apr-22	9.8	Asciidoctor-include-ext is Asciidoctor's standard include processor reimplemented as an extension. Versions	https://github.com/jirutka/asciidoctor-include-ext/commit/cbaccf3de533cbc	A-ASC-ASCI-190422/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			prior to 0.4.0, when used to render user-supplied input in AsciiDoc markup, may allow an attacker to execute arbitrary system commands on the host operating system. This attack is possible even when `allow-uri-read` is disabled! The problem has been patched in the referenced commits. **CVE ID : CVE-2022-24803**	a224bf61d0b74e4b84d41d8ee, https://github.com/jirutka/asciidoctor-include-ext/commit/c7ea001a597c7033575342c51483dab7b87ae155	
Vendor: atlasgondal					
Product: export_all_urls					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-22	6.1	The Export All URLs WordPress plugin before 4.2 does not sanitise and escape the CSV filename before outputting it back in the page, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-0892**	N/A	A-ATL-EXPO-190422/15
Cross-Site Request Forgery (CSRF)	11-Apr-22	6.5	The Export All URLs WordPress plugin before 4.3 does not have CSRF in place when exporting data, which could allow attackers to make a logged in admin export all posts and pages (including private and draft) into an arbitrary CSV	N/A	A-ATL-EXPO-190422/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file, which the attacker can then download and retrieve the list of titles for example **CVE ID : CVE-2022-0914**		
Vendor: autolabproject					
Product: autolab					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-22	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository autolab/autolab prior to 2.8.0. **CVE ID : CVE-2022-0936**	https://github.com/autolab/autolab/commit/02d76ab3737689bba95ffe9a1c69ca5166d71c6b, https://huntr.dev/bounties/90701766-bfed-409e-b3dd-6ff884373968	A-AUT-AUTO-190422/17
Vendor: baigo					
Product: baigo_cms					
Unrestricted Upload of File with Dangerous Type	06-Apr-22	7.2	A remote code execution (RCE) vulnerability in baigo CMS v3.0-alpha-2 was discovered to allow attackers to execute arbitrary code via uploading a crafted PHP file. **CVE ID : CVE-2022-26607**	N/A	A-BAI-BAIG-190422/18
Vendor: Barco					
Product: control_room_management_suite					
Improper Limitation of a	03-Apr-22	7.5	Barco Control Room Management through Suite 2.9 Build 0275	N/A	A-BAR-CONT-190422/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			was discovered to be vulnerable to directory traversal, allowing attackers to access sensitive information and components. Requests must begin with the "GET /..\.." substring. **CVE ID : CVE-2022-26233**		
Vendor: bettinivideo					
Product: sgsetup					
Use of Hard-coded Credentials	04-Apr-22	9.8	Bettini Srl GAMS Product Line v4.3.0 was discovered to re-use static SSH keys across installations, allowing unauthenticated attackers to login as root users via extracting a key from the software. **CVE ID : CVE-2022-25569**	N/A	A-BET-SGSE-190422/20
Vendor: Bigantsoft					
Product: bigant_server					
Incorrect Permission Assignment for Critical Resource	05-Apr-22	7.5	BigAnt Server v5.6.06 was discovered to contain an incorrect access control issue. **CVE ID : CVE-2022-26281**	N/A	A-BIG-BIGA-190422/21
Vendor: Bitdefender					
Product: endpoint_security_tools					
N/A	07-Apr-22	7.5	Improper Handling of Length Parameter Inconsistency	https://www.bitdefender.com/support/secu	A-BIT-ENDP-190422/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the Update Server component of Bitdefender Endpoint Security Tools (in relay role), GravityZone (in Update Server role) allows an attacker to cause a Denial-of-Service. This issue affects: Bitdefender Update Server versions prior to 3.4.0.276. Bitdefender GravityZone versions prior to 26.4-1. Bitdefender Endpoint Security Tools for Linux versions prior to 6.2.21.171. Bitdefender Endpoint Security Tools for Windows versions prior to 7.4.1.111. **CVE ID : CVE-2022-0677**	rity-advisories/improper-handling-of-length-parameter-inconsistency-vulnerability-in-bitdefender-update-server-va-10144	
Product: gravityzone					
N/A	07-Apr-22	7.5	Improper Handling of Length Parameter Inconsistency vulnerability in the Update Server component of Bitdefender Endpoint Security Tools (in relay role), GravityZone (in Update Server role) allows an attacker to cause a Denial-of-Service. This issue affects: Bitdefender	https://www.bitdefender.com/support/security-advisories/improper-handling-of-length-parameter-inconsistency-vulnerability-in-bitdefender-update-server-va-10144	A-BIT-GRAV-190422/23

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Update Server versions prior to 3.4.0.276. Bitdefender GravityZone versions prior to 26.4-1. Bitdefender Endpoint Security Tools for Linux versions prior to 6.2.21.171. Bitdefender Endpoint Security Tools for Windows versions prior to 7.4.1.111. **CVE ID : CVE-2022-0677**		
Product: update_server					
N/A	07-Apr-22	7.5	Improper Handling of Length Parameter Inconsistency vulnerability in the Update Server component of Bitdefender Endpoint Security Tools (in relay role), GravityZone (in Update Server role) allows an attacker to cause a Denial-of-Service. This issue affects: Bitdefender Update Server versions prior to 3.4.0.276. Bitdefender GravityZone versions prior to 26.4-1. Bitdefender Endpoint Security Tools for Linux versions prior to 6.2.21.171. Bitdefender Endpoint Security Tools for	https://www.bitdefender.com/support/security-advisories/improper-handling-of-length-parameter-inconsistency-vulnerability-in-bitdefender-update-server-va-10144	A-BIT-UPDA-190422/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows versions prior to 7.4.1.111. **CVE ID : CVE-2022-0677**		
Vendor: brew					
Product: mruby					
NULL Pointer Dereference	02-Apr-22	6.5	NULL Pointer Dereference in mrb_vm_exec with super in GitHub repository mruby/mruby prior to 3.2. This vulnerability is capable of making the mruby interpreter crash, thus affecting the availability of the system. **CVE ID : CVE-2022-1201**	https://huntr.dev/bounties/6f930add-c9d8-4870-ae56-d4bd8354703b, https://github.com/mruby/mruby/commit/00acae117da1b45b318dc36531a7b0021b8097ae	A-BRE-MRUB-190422/25
Vendor: buildah_project					
Product: buildah					
Incorrect Default Permissions	04-Apr-22	6.8	A flaw was found in buildah where containers were incorrectly started with non-empty default permissions. A bug was found in Moby (Docker Engine) where containers were incorrectly started with non-empty inheritable Linux process capabilities, enabling an attacker with access to programs with inheritable file	https://github.com/containers/buildah/commit/e7e55c988c05dd74005184ceb64f097a0cfe645b	A-BUI-BUIL-190422/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			capabilities to elevate those capabilities to the permitted set when execve(2) runs. This has the potential to impact confidentiality and integrity. **CVE ID : CVE-2022-27651**		
Vendor: Busybox					
Product: busybox					
N/A	03-Apr-22	9.8	BusyBox through 1.35.0 allows remote attackers to execute arbitrary code if netstat is used to print a DNS PTR record's value to a VT compatible terminal. Alternatively, the attacker could choose to change the terminal's colors. **CVE ID : CVE-2022-28391**	https://git.alpinelinux.org/aports/plain/main/busybox/0002-nslookup-sanitize-all-printed-strings-with-printable.patch , https://gitlab.alpinelinux.org/alpine/aports/-/issues/13661	A-BUS-BUSY-190422/27
Vendor: calibre-web_project					
Product: calibre-web					
Improper Access Control	03-Apr-22	4.3	Improper Access Control in GitHub repository janeczku/calibre-web prior to 0.6.16. **CVE ID : CVE-2022-0405**	https://huntr.dev/bounties/370538f6-5312-4c15-9fc0-b4c36ac236fe, https://github.com/janeczku/calibre-web/commit/3b216bfa07ec7992eff03e55d6	A-CAL-CALI-190422/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				1732af6df9bb92	
Incorrect Authorization	03-Apr-22	4.3	Improper Authorization in GitHub repository janeczku/calibre-web prior to 0.6.16. **CVE ID : CVE-2022-0406**	https://github.com/janeczku/calibre-web/commit/e0e04220109920575179a8f924543449c6de0706, https://huntr.dev/bounties/d7498799-4797-4751-b5e2-b669e729d5db	A-CAL-CALI-190422/29
Server-Side Request Forgery (SSRF)	04-Apr-22	9.9	Server-Side Request Forgery (SSRF) in GitHub repository janeczku/calibre-web prior to 0.6.18. **CVE ID : CVE-2022-0939**	https://huntr.dev/bounties/768fd7e2-a767-4d8d-a517-e9dda849c6e4, https://github.com/janeczku/calibre-web/commit/4545f4a20d9ff90b99bbd4e3e34b6de4441d6367	A-CAL-CALI-190422/30
Server-Side Request Forgery (SSRF)	04-Apr-22	9.1	Server-Side Request Forgery (SSRF) in GitHub repository janeczku/calibre-web prior to 0.6.18. **CVE ID : CVE-2022-0990**	https://github.com/janeczku/calibre-web/commit/4545f4a20d9ff90b99bbd4e3e34b6de4441d6367, https://huntr.dev/bounties/31649903-c19c-4dae-	A-CAL-CALI-190422/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				aee0-a04b095855c5	
Vendor: car_rental_system_project					
Product: car_rental_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Apr-22	8.8	Car Rental System v1.0 was discovered to contain a SQL injection vulnerability at /Car_Rental/booking.php via the id parameter. **CVE ID : CVE-2022-28000**	N/A	A-CAR-CAR_-190422/32
Vendor: Cisco					
Product: cx_cloud_agent					
Improper Control of Generation of Code ('Code Injection')	01-Apr-22	9.8	A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it. **CVE ID : CVE-2022-22965**	https://tanzu.vmware.com/security/cve-2022-22965, https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0005	A-CIS-CX_C-190422/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: identity_services_engine					
N/A	06-Apr-22	7.5	A vulnerability in the RADIUS feature of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to cause the affected system to stop processing RADIUS packets. This vulnerability is due to improper handling of certain RADIUS requests. An attacker could exploit this vulnerability by attempting to authenticate to a network or a service where the access server is using Cisco ISE as the RADIUS server. A successful exploit could allow the attacker to cause Cisco ISE to stop processing RADIUS requests, causing authentication/authorization timeouts, which would then result in legitimate requests being denied access. Note: To recover the ability to process RADIUS packets, a manual restart of the affected Policy Service Node (PSN) is required. See	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-dos-JLh9TxBp	A-CIS-IDEN-190422/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section for more information. **CVE ID : CVE-2022-20756**		
Improper Privilege Management	06-Apr-22	6.5	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information from an affected device. This vulnerability is due to improper enforcement of administrative privilege levels for high-value sensitive data. An attacker with read-only Administrator privileges to the web-based management interface on an affected device could exploit this vulnerability by browsing to a page that contains sensitive data. A successful exploit could allow the attacker to collect sensitive information regarding the configuration of the system. **CVE ID : CVE-2022-20782**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-info-exp-YXAWYP3s	A-CIS-IDEN-190422/35

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: secure_network_analytics					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-22	5.4	A vulnerability in the web-based management interface of the Network Diagrams application for Cisco Secure Network Analytics, formerly Stealthwatch Enterprise, could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user 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-2022-20741**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sna-xss-mCA9tQnJ	A-CIS-SECU-190422/36
Product: telepresence_video_communication_server					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Apr-22	7.2	Multiple vulnerabilities in the API and web-based management interfaces of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated, remote attacker with read/write privileges to the application to write files or execute arbitrary code on the underlying operating system of an affected device as the root user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20754**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-filewrite-87Q5YRk	A-CIS-TELE-190422/37
N/A	06-Apr-22	7.2	Multiple vulnerabilities in the API and web-based management interfaces of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated, remote attacker with read/write privileges to the application to write files or execute	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-filewrite-87Q5YRk	A-CIS-TELE-190422/38

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code on the underlying operating system of an affected device as the root user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20755**		
Product: ultra_cloud_core					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Apr-22	6.7	A vulnerability in the CLI of Cisco StarOS could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient input validation of CLI commands. An attacker could exploit this vulnerability by sending crafted commands to the CLI. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the root user. To exploit this vulnerability, an attacker would need to have valid administrative credentials on an affected device. **CVE ID : CVE-2022-20665**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-staros-cmdinj-759mNT4n	A-CIS-ULTR-190422/39
Product: ultra_cloud_core_-_subscriber_microservices_infrastructure					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Apr-22	7.8	A vulnerability in the Common Execution Environment (CEE) ConfD CLI of Cisco Ultra Cloud Core - Subscriber Microservices Infrastructure (SMI) software could allow an authenticated, local attacker to escalate privileges on an affected device. This vulnerability is due to insufficient access control in the affected CLI. An attacker could exploit this vulnerability by authenticating as a CEE ConfD CLI user and executing a specific CLI command. A successful exploit could allow an attacker to access privileged containers with root privileges. **CVE ID : CVE-2022-20762**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccsmi-prvesc-BQHGe4cm	A-CIS-ULTR-190422/40
Product: webex_meetings_online					
Deserialization of Untrusted Data	06-Apr-22	8.8	A vulnerability in the login authorization components of Cisco Webex Meetings could allow an authenticated, remote attacker to inject arbitrary Java code. This vulnerability is due to improper deserialization of Java	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-java-MVX6crH9	A-CIS-WEBE-190422/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code within login requests. An attacker could exploit this vulnerability by sending malicious login requests to the Cisco Webex Meetings service. A successful exploit could allow the attacker to inject arbitrary Java code and take arbitrary actions within the Cisco Webex Meetings application. **CVE ID : CVE-2022-20763**		
Product: web_security_appliance					
Improper Input Validation	06-Apr-22	5.3	A vulnerability in the Web-Based Reputation Score (WBRS) engine of Cisco AsyncOS Software for Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to bypass established web request policies and access blocked content on an affected device. This vulnerability is due to incorrect handling of certain character combinations inserted into a URL. An attacker could exploit this vulnerability by sending crafted URLs	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-swa-filter-bypass-XXXTU3X	A-CIS-WEB_-190422/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to be processed by an affected device. A successful exploit could allow the attacker to bypass the web proxy and access web content that has been blocked by policy. **CVE ID : CVE-2022-20784**		
Vendor: cocoapods					
Product: cocoapods-downloader					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	01-Apr-22	9.8	The package cocoapods-downloader before 1.6.2 are vulnerable to Command Injection via hg argument injection. When calling the download function (when using hg), the url (and/or revision, tag, branch) is passed to the hg clone command in a way that additional flags can be set. The additional flags can be used to perform a command injection. **CVE ID : CVE-2022-21223**	https://github.com/CocoaPods/cocoapods-downloader/pull/127	A-COC-COCO-190422/43
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	01-Apr-22	9.8	The package cocoapods-downloader before 1.6.0, from 1.6.2 and before 1.6.3 are vulnerable to Command Injection via git argument injection. When	https://github.com/CocoaPods/cocoapods-downloader/pull/128, https://github.com/CocoaPods/cocoapods-	A-COC-COCO-190422/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calling the Pod::Downloader.preprocess_options function and using git, both the git and branch parameters are passed to the git ls-remote subcommand in a way that additional flags can be set. The additional flags can be used to perform a command injection. **CVE ID : CVE-2022-24440**	downloader/pull/124	
Vendor: Codesys					
Product: control_for_beaglebone_sl					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a09a539ee381ca&download=	A-COD-CONT-190422/45
Product: control_for_beckhoff_cx9020					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a09a539ee381ca&download=	A-COD-CONT-190422/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: control_for_empc-a\/imx6_sl					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a09a539ee381ca&download=	A-COD-CONT-190422/47
Product: control_for_iot2000_sl					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a09a539ee381ca&download=	A-COD-CONT-190422/48
Product: control_for_linux_sl					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a09a539ee381ca&download=	A-COD-CONT-190422/49
Product: control_for_pfc100_sl					
NULL Pointer	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the	https://customers.codesys.com/index.php?eID=dumpFile&	A-COD-CONT-190422/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	t=f&f=17093&token=15cd8424832ea10dcd4873a409a539ee381ca&download=	
Product: control_for_pfc200_sl					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a539ee381ca&download=	A-COD-CONT-190422/51
Product: control_for_plcnext_sl					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a539ee381ca&download=	A-COD-CONT-190422/52
Product: control_for_raspberry_pi_sl					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash.	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a5	A-COD-CONT-190422/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22513	39ee381ca&download=	
Product: control_for_wago_touch_panels_600_sl					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a0a539ee381ca&download=	A-COD-CONT-190422/54
Product: control_rte_sl					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a0a539ee381ca&download=	A-COD-CONT-190422/55
Product: control_rte_sl_\(for_beckhoff_cx\)					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a0a539ee381ca&download=	A-COD-CONT-190422/56
Product: control_runtime_system_toolkit					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a09a539ee381ca&download=	A-COD-CONT-190422/57
Product: control_win_sl					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a09a539ee381ca&download=	A-COD-CONT-190422/58
Product: development_system					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a09a539ee381ca&download=	A-COD-DEVE-190422/59
Product: edge_gateway					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&t	A-COD-EDGE-190422/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	oken=15cd8424832ea10dcd4873a409a539ee381ca&download=	
Product: embedded_target_visu_toolkit					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a539ee381ca&download=	A-COD-EMBE-190422/61
Product: gateway					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a539ee381ca&download=	A-COD-GATE-190422/62
Product: hmi_sl					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash.	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a539ee381ca&download=	A-COD-HMI_-190422/63

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22513		
Product: remote_target_visu_toolkit					
NULL Pointer Dereference	07-Apr-22	6.5	An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash. **CVE ID : CVE-2022-22513**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a09a539ee381ca&download=	A-COD-REMO-190422/64
Vendor: college_website_content_management_system_project					
Product: college_website_content_management_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-22	5.4	A cross-site scripting (XSS) vulnerability in College Website Content Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the User Profile Name text fields. **CVE ID : CVE-2022-26615**	N/A	A-COL-COLL-190422/65
Vendor: cozmoslabs					
Product: profile_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	4.8	The Profile Builder WordPress plugin before 3.6.8 does not sanitise and escape Form Fields titles and description, which could allow high privilege user such as admin to perform Criss-Site Scripting	https://plugins.trac.wordpress.org/changeset/2690776	A-COZ-PROF-190422/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks even when unfiltered_html is disallowed **CVE ID : CVE-2022-0884**		
Vendor: Craftcms					
Product: craft_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Apr-22	6.1	Craft CMS before 3.7.29 allows XSS. **CVE ID : CVE-2022-28378**	N/A	A-CRA-CRAF-190422/67
Vendor: crun_project					
Product: crun					
Incorrect Default Permissions	04-Apr-22	7.5	A flaw was found in crun where containers were incorrectly started with non-empty default permissions. A vulnerability was found in Moby (Docker Engine) where containers were started incorrectly with non-empty inheritable Linux process capabilities. This flaw allows an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs.	https://github.com/containers/crun/commit/1aeeed2e4fdeffb4875c0d0b439915894594c8c6	A-CRU-CRUN-190422/68

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-27650		
Vendor: Cybernetikz					
Product: easy_social_icons					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-22	4.8	The Easy Social Icons WordPress plugin before 3.2.1 does not properly escape the image_file field when adding a new social icon, allowing high privileged users to inject arbitrary javascript even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-0840**	N/A	A-CYB-EASY-190422/69
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Apr-22	7.2	The Easy Social Icons WordPress plugin before 3.1.4 does not sanitize the selected_icons attribute to the cnss_widget before using it in an SQL statement, leading to a SQL injection vulnerability. **CVE ID : CVE-2022-0887**	N/A	A-CYB-EASY-190422/70
Vendor: dascomsoft					
Product: eziosuite					
Unrestricted Upload of File with Dangerous Type	06-Apr-22	8.8	eZiosuite v2.0.7 contains an authenticated arbitrary file upload via the Avatar upload functionality.	N/A	A-DAS-EZIO-190422/71

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26605		
Vendor: deepmerge-ts_project					
Product: deepmerge-ts					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	01-Apr-22	9.8	deepmerge-ts is a typescript library providing functionality to deep merging of javascript objects. deepmerge-ts is vulnerable to Prototype Pollution via file deepmerge.ts, function defaultMergeRecords(). This issue has been patched in version 4.0.2. There are no known workarounds for this issue. **CVE ID : CVE-2022-24802**	https://github.com/RebeccaStevens/deepmerge-ts/security/advisories/GHSA-r9w3-g83q-m6hq, https://github.com/RebeccaStevens/deepmerge-ts/commit/d637db7e4fb2bfb113cb4bc1c85a125936d7081b	A-DEE-DEEP-190422/72
Vendor: Dell					
Product: alienware_update					
Uncontrolled Search Path Element	01-Apr-22	7.8	Dell Command | Update, Dell Update, and Alienware Update versions prior to 4.5 contain a Local Privilege Escalation Vulnerability in the Advanced Driver Restore component. A local malicious user could potentially exploit this vulnerability, leading to privilege escalation. **CVE ID : CVE-2022-24426**	https://www.dell.com/support/kbdoc/en-us/000197723/dsa-2022-074	A-DEL-ALIE-190422/73

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: command_update					
Uncontrolled Search Path Element	01-Apr-22	7.8	Dell Command | Update, Dell Update, and Alienware Update versions prior to 4.5 contain a Local Privilege Escalation Vulnerability in the Advanced Driver Restore component. A local malicious user could potentially exploit this vulnerability, leading to privilege escalation. **CVE ID : CVE-2022-24426**	https://www.dell.com/support/kbdoc/en-us/000197723/dsa-2022-074	A-DEL-COMM-190422/74
Product: update					
Uncontrolled Search Path Element	01-Apr-22	7.8	Dell Command | Update, Dell Update, and Alienware Update versions prior to 4.5 contain a Local Privilege Escalation Vulnerability in the Advanced Driver Restore component. A local malicious user could potentially exploit this vulnerability, leading to privilege escalation. **CVE ID : CVE-2022-24426**	https://www.dell.com/support/kbdoc/en-us/000197723/dsa-2022-074	A-DEL-UPDA-190422/75
Product: wyse_device_agent					
Improper Authentication	01-Apr-22	6.7	Wyse Device Agent version 14.6.1.4 and below contain an Improper Authentication	https://www.dell.com/support/kbdoc/000196005	A-DEL-WYSE-190422/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. A malicious user could potentially exploit this vulnerability by providing invalid input in order to obtain a connection to WMS server. **CVE ID : CVE-2022-23156**		
Exposure of Sensitive Information to an Unauthorized Actor	01-Apr-22	4.4	Wyse Device Agent version 14.6.1.4 and below contain a sensitive data exposure vulnerability. A authenticated malicious user could potentially exploit this vulnerability in order to view sensitive information from the WMS Server. **CVE ID : CVE-2022-23157**	https://www.dell.com/support/kbdoc/000196005	A-DEL-WYSE-190422/77
Exposure of Sensitive Information to an Unauthorized Actor	01-Apr-22	4.4	Wyse Device Agent version 14.6.1.4 and below contain a sensitive data exposure vulnerability. A local authenticated user with standard privilege could potentially exploit this vulnerability and provide incorrect port information and get connected to valid WMS server **CVE ID : CVE-2022-23158**	https://www.dell.com/support/kbdoc/000196005	A-DEL-WYSE-190422/78

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wyse_management_suite					
Unrestricted Upload of File with Dangerous Type	01-Apr-22	7.2	Dell Wyse Management Suite versions 2.0 through 3.5.2 contain an unrestricted file upload vulnerability. A malicious user with admin privileges can exploit this vulnerability in order to execute arbitrary code on the system. **CVE ID : CVE-2022-23155**	https://www.dell.com/support/kbdoc/000195918	A-DEL-WYSE-190422/79
Vendor: deltaww					
Product: diaenergie					
Uncontrolled Search Path Element	01-Apr-22	7.8	Delta Electronics DIAEnergie (all versions prior to 1.8.02.004) are vulnerable to a DLL hijacking condition. When combined with the Incorrect Default Permissions vulnerability of 4.2.2 above, this makes it possible for an attacker to escalate privileges **CVE ID : CVE-2022-1098**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01	A-DEL-DIAE-190422/80
Vendor: dompdf_project					
Product: dompdf					
Improper Neutralization of Special Elements in Output	03-Apr-22	9.8	Dompdf 1.2.1 allows remote code execution via a .php file in the src:url field of an @font-face Cascading Style	https://github.com/dompdf/dompdf/commit/4c70e1025bcd9b7694b95dd552499bd83c	A-DOM-DOMP-190422/81

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Used by a Downstream Component ('Injection')			Sheets (CSS) statement (within an HTML input file). **CVE ID : CVE-2022-28368**	d6141d, https://github.com/dompdf/dompdf/pull/2808, https://github.com/dompdf/dompdf/issues/2598	
Vendor: ecommerce-website_product					
Product: ecommerce-website					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	4.8	A cross-site scripting (XSS) vulnerability in /public/admin/index.php?add_user at Ecommerce-Website v1.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the username text field. **CVE ID : CVE-2022-27436**	N/A	A-ECO-ECOM-190422/82
Vendor: ecommerce-website_project					
Product: ecommerce-website					
Unrestricted Upload of File with Dangerous Type	08-Apr-22	8.8	Ecommece-Website v1.1.0 was discovered to contain an arbitrary file upload vulnerability via /admin/index.php?slides. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-27346**	N/A	A-ECO-ECOM-190422/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	08-Apr-22	9.8	Ecommerce-Website v1 was discovered to contain an arbitrary file upload vulnerability via /customer_register.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-27357**	N/A	A-ECO-ECOM-190422/84
Unrestricted Upload of File with Dangerous Type	04-Apr-22	8.8	An unrestricted file upload at /public/admin/index.php?add_product of Ecommerce-Website v1.1.0 allows attackers to upload a webshell via the Product Image component. **CVE ID : CVE-2022-27435**	N/A	A-ECO-ECOM-190422/85
Vendor: elbtide					
Product: advanced_booking_calendar					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Apr-22	7.2	The Advanced Booking Calendar WordPress plugin before 1.7.1 does not sanitise and escape the id parameter when editing Calendars, which could allow high privilege users such as admin to perform SQL injection attacks **CVE ID : CVE-2022-1006**	https://wpscan.com/vulnerability/c5569317-b8c8-4524-8375-3e2369bdcc68, https://plugins.trac.wordpress.org/changeset/2695427	A-ELB-ADVA-190422/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-22	6.1	The Advanced Booking Calendar WordPress plugin before 1.7.1 does not sanitise and escape the room parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting issue **CVE ID : CVE-2022-1007**	https://wpscan.com/vulnerability/6f5b764b-d13b-4371-9cc5-91204d9d6358, https://plugins.trac.wordpress.org/changeset/2695427	A-ELB-ADVA-190422/87
Vendor: employee_performance_evaluation_project					
Product: employee_performance_evaluation					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-22	9.8	Employee Performance Evaluation v1.0 was discovered to contain a SQL injection vulnerability via the email parameter. **CVE ID : CVE-2022-27123**	N/A	A-EMP-EMPL-190422/88
Vendor: eyecix					
Product: careerfy					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	6.1	There is a XSS vulnerability in Careerfy. **CVE ID : CVE-2022-1169**	N/A	A-EYE-CARE-190422/89
Product: jobsearch_wp_job_board					
Improper Neutralization of Input	04-Apr-22	6.1	There is a Cross-Site Scripting vulnerability in the JobSearch WP	N/A	A-EYE-JOBS-190422/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			JobSearch WordPress plugin before 1.5.1. **CVE ID : CVE-2022-1168**		
Vendor: febs-security_project					
Product: febs-security					
Incorrect Default Permissions	10-Apr-22	5.4	Insecure permissions configured in the userid parameter at /user/getuserprofile of FEBS-Security v1.0 allows attackers to access and arbitrarily modify users' personal information. **CVE ID : CVE-2022-27958**	N/A	A-FEB-FEBS-190422/91
Vendor: finn					
Product: podium_layout					
N/A	06-Apr-22	7.5	Podium is a library for building micro frontends. @podium/layout is a module for building a Podium layout server, and @podium/proxy is a module for proxying HTTP requests from a layout server to a podlet server. In @podium/layout prior to version 4.6.110 and @podium/proxy prior to version 4.2.74, an attacker using the `Trailer` header as part of the request against proxy endpoints has the	https://github.com/podium-lib/proxy/security/advisories/GHSA-3hjg-vc7r-rcrw, https://github.com/podium-lib/proxy/commit/9698a40df081217ce142d4de71f929baaa339cdf, https://github.com/podium-lib/layout/commit/fe43e655432b0a5f07b6475f67babcc2588fb039	A-FIN-PODI-190422/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ability to take down the server. All Podium layouts that include podlets with proxy endpoints are affected. `@podium/layout`, which is the main way developers/users are vulnerable to this exploit, has been patched in version `4.6.110`. All earlier versions are vulnerable.`@podium /proxy`, which is the source of the vulnerability and is used by `@podium/layout` has been patched in version `4.2.74`. All earlier versions are vulnerable. It is not easily possible to work around this issue without upgrading. **CVE ID : CVE-2022-24822**		
Product: podium_proxy					
N/A	06-Apr-22	7.5	Podium is a library for building micro frontends. @podium/layout is a module for building a Podium layout server, and @podium/proxy is a module for proxying HTTP requests from a layout server to a podlet server. In	https://github.com/podium-lib/proxy/security/advisories/GHSA-3hjg-vc7r-rcrw, https://github.com/podium-lib/proxy/commit/9698a40df081217ce142d4de71f929baa	A-FIN-PODI-190422/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			@podium/layout prior to version 4.6.110 and @podium/proxy prior to version 4.2.74, an attacker using the `Trailer` header as part of the request against proxy endpoints has the ability to take down the server. All Podium layouts that include podlets with proxy endpoints are affected. `@podium/layout`, which is the main way developers/users are vulnerable to this exploit, has been patched in version `4.6.110`. All earlier versions are vulnerable.`@podium/proxy`, which is the source of the vulnerability and is used by `@podium/layout` has been patched in version `4.2.74`. All earlier versions are vulnerable. It is not easily possible to work around this issue without upgrading. **CVE ID : CVE-2022-24822**	a339cdf, https://github.com/podium-lib/layout/commit/fe43e655432b0a5f07b6475f67babcc2588fb039	
Vendor: Foliovision					
Product: fv_flowplayer_video_player					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	5.4	Authenticated Persistent Cross-Site Scripting (XSS) vulnerability in FV Flowplayer Video Player (WordPress plugin) versions <= 7.5.18.727 via &fv_wp_flowplayer_field_splash parameter. **CVE ID : CVE-2022-25613**	https://patchstack.com/database/vulnerability/fv-wordpress-flowplayer/wordpress-fv-flowplayer-video-player-plugin-7-5-18-727-authenticated-persistent-cross-site-scripting-xss-vulnerability, https://wordpress.org/plugins/fv-wordpress-flowplayer/#developers	A-FOL-FV_F-190422/94
Vendor: forcepoint					
Product: one_endpoint					
Incorrect Authorization	04-Apr-22	6	Forcepoint One Endpoint prior to version 22.01 installed on Microsoft Windows is vulnerable to registry key tampering by users with Administrator privileges. This could result in a user disabling anti-tampering mechanisms which would then allow the user to disable Forcepoint One Endpoint and the	https://help.forcepoint.com/security/CVE/CVE-2022-27608.html	A-FOR-ONE_-190422/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protection offered by it. **CVE ID : CVE-2022-27608**		
Incorrect Authorization	04-Apr-22	6	Forcepoint One Endpoint prior to version 22.01 installed on Microsoft Windows does not provide sufficient anti-tampering protection of services by users with Administrator privileges. This could result in a user disabling Forcepoint One Endpoint and the protection offered by it. **CVE ID : CVE-2022-27609**	https://help.forcepoint.com/security/CVE/CVE-2022-27609.html	A-FOR-ONE_-190422/96
Vendor: formbuilder_project					
Product: formbuilder					
Cross-Site Request Forgery (CSRF)	04-Apr-22	6.5	The FormBuilder WordPress plugin through 1.08 does not have CSRF checks in place when creating/updating and deleting forms, and does not sanitise as well as escape its form field values. As a result, attackers could make logged in admin update and delete arbitrary forms via a CSRF attack, and put Cross-Site Scripting payloads in them.	N/A	A-FOR-FORM-190422/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0830		
Vendor: Fortinet					
Product: fortiedr					
Use of Hard-coded Credentials	06-Apr-22	7.8	A use of hard-coded cryptographic key vulnerability [CWE-321] in the registration mechanism of FortiEDR collectors versions 5.0.2, 5.0.1, 5.0.0, 4.0.0 may allow a local attacker to disable and uninstall the collectors from the end-points within the same deployment. **CVE ID : CVE-2022-23440**	https://fortiguard.com/psirt/FG-IR-22-018	A-FOR-FORT-190422/98
Use of Hard-coded Credentials	06-Apr-22	9.1	A use of hard-coded cryptographic key vulnerability [CWE-321] in FortiEDR versions 5.0.2, 5.0.1, 5.0.0, 4.0.0 may allow an unauthenticated attacker on the network to disguise as and forge messages from other collectors. **CVE ID : CVE-2022-23441**	https://fortiguard.com/psirt/FG-IR-22-019	A-FOR-FORT-190422/99
N/A	06-Apr-22	4.4	A improper control of a resource through its lifetime in Fortinet FortiEDR version 5.0.3 and earlier allows attacker to make the whole application unresponsive via	https://fortiguard.com/psirt/FG-IR-22-052	A-FOR-FORT-190422/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			changing its root directory access permission. **CVE ID : CVE-2022-23446**		
Vendor: Fujitsu					
Product: plugfree_network					
Unquoted Search Path or Element	11-Apr-22	7.8	In Fujitsu PlugFree Network <= 7.3.0.3, an Unquoted service path in PFNService.exe software allows a local attacker to potentially escalate privileges to system level. **CVE ID : CVE-2022-27089**	N/A	A-FUJ-PLUG-190422/101
Vendor: fullpage_project					
Product: fullpage					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	11-Apr-22	9.8	Prototype Pollution in GitHub repository alvarotrigo/fullpage.js prior to 4.0.2. **CVE ID : CVE-2022-1295**	https://huntr.dev/bounties/3b9d450c-24ac-4037-b04d-4d4dafbf593a, https://github.com/alvarotrigo/fullpage.js/commit/bf62492a22e5d296e63c3ed918a42fc5645a0d48	A-FUL-FULL-190422/102
Vendor: getbootstrap					
Product: bootstrap					
Improper Neutralization of Input	08-Apr-22	6.1	Bootstrap v3.1.11 and v3.3.7 was discovered to contain a cross-site scripting (XSS)	N/A	A-GET-BOOT-190422/103

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			vulnerability via the Title parameter in /vendor/views/add_product.php. **CVE ID : CVE-2022-26624**		
Vendor: gimmal					
Product: sherpa_connector_service					
Unquoted Search Path or Element	05-Apr-22	7.8	There is an unquoted service path in Sherpa Connector Service (SherpaConnectorService.exe) 2020.2.20328.2050. This might allow a local user to escalate privileges by creating a "C:\Program Files\Sherpa Software\Sherpa.exe" file. **CVE ID : CVE-2022-23909**	N/A	A-GIM-SHER-190422/104
Vendor: Github					
Product: enterprise_server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Apr-22	8.8	A path traversal vulnerability was identified in GitHub Enterprise Server management console that allowed the bypass of CSRF protections. This could potentially lead to privilege escalation. To exploit this vulnerability, an attacker would need to target a user that was actively logged into the management	https://docs.github.com/en/enterprise-server@3.4/admin/release-notes#3.4.1, https://docs.github.com/en/enterprise-server@3.2/admin/release-notes#3.2.11, https://docs.github.com/en/enterprise-server@3.3/ad	A-GIT-ENTE-190422/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			console. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.5 and was fixed in versions 3.1.19, 3.2.11, 3.3.6, 3.4.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2022-23732**	min/release-notes#3.3.6	
Vendor: Gitlab					
Product: gitlab					
Incorrect Authorization	01-Apr-22	4.3	Improper access control in GitLab CE/EE versions 12.4 to 14.5.4, 14.5 to 14.6.4, and 12.6 to 14.7.1 allows project non-members to retrieve the service desk email address **CVE ID : CVE-2022-0373**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0373.json	A-GIT-GITL-190422/106
Incorrect Authorization	01-Apr-22	4.3	Improper access control in Gitlab CE/EE versions 12.7 to 14.5.4, 14.6 to 14.6.4, and 14.7 to 14.7.1 allowed for project non-members to retrieve issue details when it was linked to an item from the vulnerability dashboard. **CVE ID : CVE-2022-0390**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0390.json	A-GIT-GITL-190422/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	01-Apr-22	7.6	A DNS rebinding vulnerability in the Irker IRC Gateway integration in all versions of GitLab CE/EE since version 7.9 allows an attacker to trigger Server Side Request Forgery (SSRF) attacks. **CVE ID : CVE-2022-0425**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0425.json	A-GIT-GITL-190422/108
Uncontrolled Resource Consumption	01-Apr-22	5.7	An issue has been discovered in GitLab CE/EE affecting all versions starting with 8.15 . It was possible to trigger a DOS by using the math feature with a specific formula in issue comments. **CVE ID : CVE-2022-0489**	https://gitlab.com/gitlab-org/gitlab/-/issues/341832, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0489.json	A-GIT-GITL-190422/109
Incorrect Authorization	04-Apr-22	4.3	Incorrect authorization in the Asana integration's branch restriction feature in all versions of GitLab CE/EE starting from version 7.8.0 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 makes it possible to close Asana tasks from unrestricted branches. **CVE ID : CVE-2022-0740**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0740.json	A-GIT-GITL-190422/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	01-Apr-22	7.5	Improper input validation in all versions of GitLab CE/EE using sendmail to send emails allowed an attacker to steal environment variables via specially crafted email addresses. **CVE ID : CVE-2022-0741**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0741.json	A-GIT-GITL-190422/111
Uncontrolled Resource Consumption	04-Apr-22	4.3	Adding a very large number of tags to a runner in GitLab CE/EE affecting all versions prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allows an attacker to impact the performance of GitLab **CVE ID : CVE-2022-1099**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1099.json	A-GIT-GITL-190422/112
Missing Release of Resource after Effective Lifetime	04-Apr-22	4.3	A potential DOS vulnerability was discovered in GitLab CE/EE affecting all versions from 13.1 prior to 14.7.7, 14.8.0 prior to 14.8.5, and 14.9.0 prior to 14.9.2. The api to update an asset as a link from a release had a regex check which caused exponential number of backtracks for certain user supplied values resulting in high CPU usage.	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1100.json	A-GIT-GITL-190422/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1100		
Incorrect Authorization	04-Apr-22	4.3	An improper access control vulnerability in GitLab CE/EE affecting all versions from 13.11 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allows an unauthorized user to access pipeline analytics even when public pipelines are disabled **CVE ID : CVE-2022-1105**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1105.json	A-GIT-GITL-190422/114
Exposure of Resource to Wrong Sphere	04-Apr-22	2.7	A business logic error in Project Import in GitLab CE/EE versions 14.9 prior to 14.9.2, 14.8 prior to 14.8.5, and 14.0 prior to 14.7.7 under certain conditions caused imported projects to show an incorrect user in the 'Access Granted' column in the project membership pages **CVE ID : CVE-2022-1111**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1111.json	A-GIT-GITL-190422/115
Generation of Error Message Containing Sensitive Information	04-Apr-22	6.5	Missing filtering in an error message in GitLab CE/EE affecting all versions prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 exposed sensitive information when an	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1120.json	A-GIT-GITL-190422/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			include directive fails in the CI/CD configuration. **CVE ID : CVE-2022-1120**		
Allocation of Resources Without Limits or Throttling	04-Apr-22	5.3	A lack of appropriate timeouts in GitLab Pages included in GitLab CE/EE all versions prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allows an attacker to cause unlimited resource consumption. **CVE ID : CVE-2022-1121**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1121.json	A-GIT-GITL-190422/117
Improper Authentication	04-Apr-22	6.5	Improper authorization in GitLab Pages included with GitLab CE/EE affecting all versions from 11.5 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allowed an attacker to steal a user's access token on an attacker-controlled private GitLab Pages website and reuse that token on the victim's other private websites **CVE ID : CVE-2022-1148**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1148.json	A-GIT-GITL-190422/118
Use of Hard-coded Credentials	04-Apr-22	9.8	A hardcoded password was set for accounts registered using an OmniAuth provider (e.g. OAuth,	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-	A-GIT-GITL-190422/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LDAP, SAML) in GitLab CE/EE versions 14.7 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allowing attackers to potentially take over accounts **CVE ID : CVE-2022-1162**	2022-1162.json	
Uncontrolled Resource Consumption	04-Apr-22	7.5	A potential DoS vulnerability was discovered in Gitlab CE/EE versions 13.7 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 allowed an attacker to trigger high CPU usage via a special crafted input added in Issues, Merge requests, Milestones, Snippets, Wiki pages, etc. **CVE ID : CVE-2022-1174**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1174.json	A-GIT-GITL-190422/120
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	6.1	Improper neutralization of user input in GitLab CE/EE versions 14.4 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 allowed an attacker to exploit XSS by	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1175.json	A-GIT-GITL-190422/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injecting HTML in notes. **CVE ID : CVE-2022-1175**		
Uncontrolled Resource Consumption	04-Apr-22	6.5	A denial of service vulnerability when rendering RDoc files in GitLab CE/EE versions 10 to 14.7.7, 14.8.0 to 14.8.5, and 14.9.0 to 14.9.2 allows an attacker to crash the GitLab web application with a maliciously crafted RDoc file **CVE ID : CVE-2022-1185**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1185.json	A-GIT-GITL-190422/122
Server-Side Request Forgery (SSRF)	04-Apr-22	5.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.1 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 where a blind SSRF attack through the repository mirroring feature was possible. **CVE ID : CVE-2022-1188**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1188.json	A-GIT-GITL-190422/123
N/A	04-Apr-22	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.2 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1189.json	A-GIT-GITL-190422/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that allowed for an unauthorised user to read the the approval rules of a private project. **CVE ID : CVE-2022-1189**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	5.4	Improper handling of user input in GitLab CE/EE versions 8.3 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allowed an attacker to exploit a stored XSS by abusing multi-word milestone references in issue descriptions, comments, etc. **CVE ID : CVE-2022-1190**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1190.json	A-GIT-GITL-190422/125
Vendor: gnuboard					
Product: gnuboard5					
Exposure of Private Personal Information to an Unauthorized Actor	11-Apr-22	7.5	Exposure of Private Personal Information to an Unauthorized Actor in GitHub repository gnuboard/gnuboard5 prior to and including 5.5.5. A vulnerability in gnuboard v5.5.5 and below uses weak encryption algorithms leading to sensitive information exposure. This allows an attacker to derive the email address of any user, including when the 'Let others	https://huntr.dev/bounties/c8c2c3e1-67d0-4a11-a4d4-11af567a9ebb	A-GNU-GNUB-190422/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			see my information.' box is ticked off. **CVE ID : CVE-2022-1252**		
Vendor: Google					
Product: chrome					
Use After Free	05-Apr-22	9.6	Use after free in Safe Browsing in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2022-0452**	https://crbug.com/1284584, https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-190422/127
Use After Free	05-Apr-22	8.8	Use after free in Reader Mode in Google Chrome prior to 98.0.4758.80 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0453**	https://crbug.com/1284916, https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-190422/128
Out-of-bounds Write	05-Apr-22	8.8	Heap buffer overflow in ANGLE in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0454**	https://crbug.com/1287962, https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-190422/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-Apr-22	6.5	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 98.0.4758.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2022-0455**	https://crbug.com/1270593, https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-190422/130
Use After Free	05-Apr-22	8.8	Use after free in Web Search in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via profile destruction. **CVE ID : CVE-2022-0456**	https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html, https://crbug.com/1289523	A-GOO-CHRO-190422/131
Access of Resource Using Incompatible Type ('Type Confusion')	05-Apr-22	8.8	Type confusion in V8 in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0457**	https://crbug.com/1274445, https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-190422/132
Use After Free	05-Apr-22	8.8	Use after free in Thumbnail Tab Strip in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	https://crbug.com/1267060, https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-190422/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0458		
Use After Free	05-Apr-22	8.8	Use after free in Screen Capture in Google Chrome prior to 98.0.4758.80 allowed a remote attacker who had compromised the renderer process and convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0459**	https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html, https://crbug.com/1244205	A-GOO-CHRO-190422/134
Use After Free	05-Apr-22	8.8	Use after free in Window Dialogue in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0460**	https://crbug.com/1250227, https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-190422/135
Exposure of Resource to Wrong Sphere	05-Apr-22	6.5	Policy bypass in COOP in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to bypass iframe sandbox via a crafted HTML page. **CVE ID : CVE-2022-0461**	https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html, https://crbug.com/1256823	A-GOO-CHRO-190422/136
N/A	05-Apr-22	6.5	Inappropriate implementation in Scroll in Google Chrome prior to	https://crbug.com/1270470, https://chromereleases.googl	A-GOO-CHRO-190422/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			98.0.4758.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2022-0462**	eblog.com/2022/02/stable-channel-update-for-desktop.html	
Use After Free	05-Apr-22	8.8	Use after free in Accessibility in Google Chrome prior to 98.0.4758.80 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via user interaction. **CVE ID : CVE-2022-0463**	https://crbug.com/1268240, https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-190422/138
Use After Free	05-Apr-22	8.8	Use after free in Accessibility in Google Chrome prior to 98.0.4758.80 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via user interaction. **CVE ID : CVE-2022-0464**	https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html, https://crbug.com/1270095	A-GOO-CHRO-190422/139
Use After Free	05-Apr-22	8.8	Use after free in Extensions in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit	https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html,	A-GOO-CHRO-190422/140

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			heap corruption via user interaction. **CVE ID : CVE-2022-0465**	https://crbug.com/1281941	
N/A	05-Apr-22	9.6	Inappropriate implementation in Extensions Platform in Google Chrome prior to 98.0.4758.80 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2022-0466**	https://crbug.com/1115460, https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-190422/141
N/A	05-Apr-22	8.8	Inappropriate implementation in Pointer Lock in Google Chrome on Windows prior to 98.0.4758.80 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2022-0467**	https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html, https://crbug.com/1239496	A-GOO-CHRO-190422/142
Use After Free	05-Apr-22	8.8	Use after free in Payments in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0468**	https://crbug.com/1252716, https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-190422/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	05-Apr-22	8.8	Use after free in Cast in Google Chrome prior to 98.0.4758.80 allowed a remote attacker who convinced a user to engage in specific interactions to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0469**	https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html, https://crbug.com/1279531	A-GOO-CHRO-190422/144
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-Apr-22	8.8	Out of bounds memory access in V8 in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0470**	https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html, https://crbug.com/1269225	A-GOO-CHRO-190422/145
Use After Free	05-Apr-22	8.8	Use after free in File Manager in Google Chrome on Chrome OS prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0603**	https://crbug.com/1290008, https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html	A-GOO-CHRO-190422/146
Out-of-bounds Write	05-Apr-22	8.8	Heap buffer overflow in Tab Groups in Google Chrome prior to 98.0.4758.102 allowed an attacker who convinced a user	https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-	A-GOO-CHRO-190422/147

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to install a malicious extension and engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0604**	desktop_14.html, https://crbug.com/1273397	
Use After Free	05-Apr-22	8.8	Use after free in Webstore API in Google Chrome prior to 98.0.4758.102 allowed an attacker who convinced a user to install a malicious extension and convinced a user to enage in specific user interaction to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0605**	https://crbug.com/1286940, https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html	A-GOO-CHRO-190422/148
Use After Free	05-Apr-22	8.8	Use after free in ANGLE in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0606**	https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html, https://crbug.com/1288020	A-GOO-CHRO-190422/149
Use After Free	05-Apr-22	8.8	Use after free in GPU in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially	https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-	A-GOO-CHRO-190422/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0607**	desktop_14.html, https://crbug.com/1250655	
Integer Overflow or Wraparound	05-Apr-22	8.8	Integer overflow in Mojo in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0608**	https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html, https://crbug.com/1270333	A-GOO-CHRO-190422/151
Use After Free	05-Apr-22	8.8	Use after free in Animation in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0609**	https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html, https://crbug.com/1296150	A-GOO-CHRO-190422/152
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-Apr-22	8.8	Inappropriate implementation in Gamepad API in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0610**	https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html, https://crbug.com/1285449	A-GOO-CHRO-190422/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Apr-22	8.8	Heap buffer overflow in ANGLE in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0789**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1289383	A-GOO-CHRO-190422/154
Use After Free	05-Apr-22	9.6	Use after free in Cast UI in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2022-0790**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1274077	A-GOO-CHRO-190422/155
Use After Free	05-Apr-22	8.8	Use after free in Omnibox in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via user interactions. **CVE ID : CVE-2022-0791**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1278322	A-GOO-CHRO-190422/156
Out-of-bounds Read	05-Apr-22	6.5	Out of bounds read in ANGLE in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-	A-GOO-CHRO-190422/157

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0792**	desktop.html, https://crbug.com/1285885	
Use After Free	05-Apr-22	6.5	Use after free in Cast in Google Chrome prior to 99.0.4844.51 allowed an attacker who convinced a user to install a malicious extension and engage in specific user interaction to potentially exploit heap corruption via a crafted Chrome Extension. **CVE ID : CVE-2022-0793**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1291728	A-GOO-CHRO-190422/158
Use After Free	05-Apr-22	8.8	Use after free in WebShare in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0794**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1294097	A-GOO-CHRO-190422/159
Access of Resource Using Incompatible Type ('Type Confusion')	05-Apr-22	8.8	Type confusion in Blink Layout in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1282782	A-GOO-CHRO-190422/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0795		
Use After Free	05-Apr-22	8.8	Use after free in Media in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0796**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1295786	A-GOO-CHRO-190422/161
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-Apr-22	8.8	Out of bounds memory access in Mojo in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. **CVE ID : CVE-2022-0797**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1281908	A-GOO-CHRO-190422/162
Use After Free	05-Apr-22	8.8	Use after free in MediaStream in Google Chrome prior to 99.0.4844.51 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. **CVE ID : CVE-2022-0798**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1283402	A-GOO-CHRO-190422/163
Improper Privilege	05-Apr-22	8.8	Insufficient policy enforcement in Installer in Google Chrome on Windows	https://chromereleases.googleblog.com/2022/03/stable-	A-GOO-CHRO-190422/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			prior to 99.0.4844.51 allowed a remote attacker to perform local privilege escalation via a crafted offline installer file. **CVE ID : CVE-2022-0799**	channel-update-for-desktop.html, https://crbug.com/1279188	
Out-of-bounds Write	05-Apr-22	8.8	Heap buffer overflow in Cast UI in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0800**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1242962	A-GOO-CHRO-190422/165
N/A	05-Apr-22	6.5	Inappropriate implementation in Full screen mode in Google Chrome on Android prior to 99.0.4844.51 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2022-0802**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1270052	A-GOO-CHRO-190422/166
Incorrect Permission Assignment for Critical Resource	05-Apr-22	6.5	Inappropriate implementation in Permissions in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to tamper with the	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html,	A-GOO-CHRO-190422/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2022-0803**	https://crbug.com/1280233	
N/A	05-Apr-22	6.5	Inappropriate implementation in Full screen mode in Google Chrome on Android prior to 99.0.4844.51 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2022-0804**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1264561	A-GOO-CHRO-190422/168
Use After Free	05-Apr-22	8.8	Use after free in Browser Switcher in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via user interaction. **CVE ID : CVE-2022-0805**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1290700	A-GOO-CHRO-190422/169
Exposure of Resource to Wrong Sphere	05-Apr-22	6.5	Data leak in Canvas in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in screen sharing to potentially leak cross-origin data	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1283434	A-GOO-CHRO-190422/170

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via a crafted HTML page. **CVE ID : CVE-2022-0806**		
N/A	05-Apr-22	6.5	Inappropriate implementation in Autofill in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2022-0807**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1287364	A-GOO-CHRO-190422/171
Use After Free	05-Apr-22	8.8	Use after free in Chrome OS Shell in Google Chrome on Chrome OS prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in a series of user interaction to potentially exploit heap corruption via user interactions. **CVE ID : CVE-2022-0808**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1292271	A-GOO-CHRO-190422/172
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-Apr-22	8.8	Out of bounds memory access in WebXR in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0809**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1293428	A-GOO-CHRO-190422/173
Vendor: gpac					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: gpac					
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Apr-22	5.5	Inf loop in GitHub repository gpac/gpac prior to 2.1.0-DEV. **CVE ID : CVE-2022-1222**	https://github.com/gpac/gpac/commit/7f060bbb72966cae80d6fee338d0b07fa3fc06e1 , https://huntr.dev/bounties/f8cb85b8-7ff3-47f1-a9a6-7080eb371a3d	A-GPA-GPAC-190422/174
Out-of-bounds Write	08-Apr-22	5.5	GPAC mp4box 1.1.0-DEV-rev1727-g8be34973d-master has a stack-overflow vulnerability in function gf_isom_get_sample_for_movie_time of mp4box. **CVE ID : CVE-2022-27145**	N/A	A-GPA-GPAC-190422/175
Out-of-bounds Write	08-Apr-22	5.5	GPAC mp4box 1.1.0-DEV-rev1759-geb2d1e6dd-has a heap-buffer-overflow vulnerability in function gf_isom_apple_enum_tag. **CVE ID : CVE-2022-27146**	N/A	A-GPA-GPAC-190422/176
Use After Free	08-Apr-22	5.5	GPAC mp4box 1.1.0-DEV-rev1727-g8be34973d-master has a use-after-free vulnerability in function gf_node_get_attribute_by_tag.	N/A	A-GPA-GPAC-190422/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-27147		
Integer Overflow or Wraparound	08-Apr-22	5.5	GPAC mp4box 1.1.0-DEV-rev1663-g881c6a94a-master is vulnerable to Integer Overflow. **CVE ID : CVE-2022-27148**	N/A	A-GPA-GPAC-190422/178
Vendor: halo					
Product: halo					
Unrestricted Upload of File with Dangerous Type	05-Apr-22	7.5	Halo Blog CMS v1.4.17 was discovered to allow attackers to upload arbitrary files via the Attachment Upload function. **CVE ID : CVE-2022-26619**	N/A	A-HAL-HALO-190422/179
Vendor: HP					
Product: oneview					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	6.1	A remote cross-site scripting (xss) vulnerability was discovered in HPE OneView version(s): Prior to 6.6. HPE has provided a software update to resolve this vulnerability in HPE OneView. **CVE ID : CVE-2022-23697**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn04252en_us	A-HP-ONEV-190422/180
N/A	04-Apr-22	7.5	A remote unauthenticated disclosure of information vulnerability was discovered in HPE	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	A-HP-ONEV-190422/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OneView version(s): Prior to 6.6. HPE has provided a software update to resolve this vulnerability in HPE OneView. **CVE ID : CVE-2022-23698**	hpesbgn04252 en_us	
Improper Authentication	04-Apr-22	7.8	A local authentication restriction bypass vulnerability was discovered in HPE OneView version(s): Prior to 6.6. HPE has provided a software update to resolve this vulnerability in HPE OneView. **CVE ID : CVE-2022-23699**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn04252en_us	A-HP-ONEV-190422/182
Incorrect Authorization	04-Apr-22	5.5	A local unauthorized read access to files vulnerability was discovered in HPE OneView version(s): Prior to 6.6. HPE has provided a software update to resolve this vulnerability in HPE OneView. **CVE ID : CVE-2022-23700**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn04252en_us	A-HP-ONEV-190422/183
Vendor: htmldoc_project					
Product: htmldoc					
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Apr-22	5.5	In HTMLDOC 1.9.14, an infinite loop in the gif_read_lzw function can lead to a pointer arbitrarily pointing to heap memory and	https://github.com/michaelrsweet/htmldoc/issues/470	A-HTM-HTML-190422/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a buffer overflow. **CVE ID : CVE-2022-24191**		
Vendor: IBM					
Product: app_connect_enterprise_certified_container					
Allocation of Resources Without Limits or Throttling	01-Apr-22	6.5	IBM App Connect Enterprise Certified Container Dashboard UI (IBM App Connect Enterprise Certified Container 1.5, 2.0, 2.1, 3.0, and 3.1) may be vulnerable to denial of service due to excessive rate limiting. **CVE ID : CVE-2022-22404**	https://exchange.xforce.ibmcloud.com/vulnerabilities/222575, https://www.ibm.com/support/pages/node/6568359	A-IBM-APP_-190422/185
Product: partner_engagement_manager					
Improper Privilege Management	01-Apr-22	6.2	IBM SterlingPartner Engagement Manager 6.2.0 could allow a malicious user to elevate their privileges and perform unintended operations to another users data. IBM X-Force ID: 218871. **CVE ID : CVE-2022-22328**	https://www.ibm.com/support/pages/node/6568297, https://exchange.xforce.ibmcloud.com/vulnerabilities/218871	A-IBM-PART-190422/186
Exposure of Resource to Wrong Sphere	01-Apr-22	7.1	IBM SterlingPartner Engagement Manager 6.2.0 could allow a remote authenticated attacker to obtain sensitive information or modify user details caused by an insecure direct object	https://www.ibm.com/support/pages/node/6568299, https://exchange.xforce.ibmcloud.com/vulnerabilities/219130	A-IBM-PART-190422/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability (IDOR). IBM X-Force ID: 219130. **CVE ID : CVE-2022-22331**		
Operation on a Resource after Expiration or Release	01-Apr-22	7.5	IBM Sterling Partner Engagement Manager 6.2.0 could allow an attacker to impersonate another user due to missing revocation mechanism for the JWT token. IBM X-Force ID: 219131. **CVE ID : CVE-2022-22332**	https://exchange.xforce.ibmcloud.com/vulnerabilities/219131, https://www.ibm.com/support/pages/node/6568301	A-IBM-PART-190422/188
Product: planning_analytics					
Server-Side Request Forgery (SSRF)	08-Apr-22	7.3	IBM Planning Analytics 2.0 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 219736. **CVE ID : CVE-2022-22339**	https://exchange.xforce.ibmcloud.com/vulnerabilities/219736, https://www.ibm.com/support/pages/node/6565099	A-IBM-PLAN-190422/189
Product: urbancode_deploy					
Use of a Broken or Risky Cryptograp	01-Apr-22	7.5	IBM UrbanCode Deploy (UCD) 7.0.5, 7.1.0, 7.1.1, and 7.1.2 uses weaker than	https://www.ibm.com/support/pages/node/6568551,	A-IBM-URBA-190422/190

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
hic Algorithm			expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 218859. **CVE ID : CVE-2022-22327**	https://exchange.xforce.ibmcloud.com/vulnerabilities/218859	
Product: watson_query					
N/A	06-Apr-22	7.2	IBM Watson Query with Cloud Pak for Data as a Service could allow an authenticated user to obtain sensitive information that would allow them to examine or alter system configurations or data sources connected to the service. IBM X-Force ID: 222763. **CVE ID : CVE-2022-22410**	https://exchange.xforce.ibmcloud.com/vulnerabilities/222763, https://www.ibm.com/support/pages/node/6569235	A-IBM-WATS-190422/191
Vendor: icehrm					
Product: icehrm					
Cross-Site Request Forgery (CSRF)	08-Apr-22	6.5	A Cross-Site Request Forgery (CSRF) in IceHrm 31.0.0.OS allows attackers to delete arbitrary users or achieve account takeover via the app/service.php URI. **CVE ID : CVE-2022-26588**	https://medium.com/@devansh3008/csrf-in-icehrm-31-0-0-0s-in-delete-user-endpoint-86a39ecf253f	A-ICE-ICEH-190422/192
Vendor: idearespa					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: reftree					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Apr-22	6.5	A directory traversal vulnerability in IdeaRE RefTree before 2021.09.17 allows remote authenticated users to download arbitrary .dwg files from a remote server by specifying an absolute or relative path when invoking the affected DownloadDwg endpoint. An attack uses the path field to CaddemServiceJS/CaddemService.svc/rest/DownloadDwg. **CVE ID : CVE-2022-27248**	N/A	A-IDE-REFT-190422/193
Unrestricted Upload of File with Dangerous Type	03-Apr-22	8.8	An unrestricted file upload vulnerability in IdeaRE RefTree before 2021.09.17 allows remote authenticated users to execute arbitrary code by using UploadDwg to upload a crafted aspx file to the web root, and then visiting the URL for this aspx resource. **CVE ID : CVE-2022-27249**	N/A	A-IDE-REFT-190422/194
Vendor: Impresscms					
Product: impresscms					
Improper Neutralization of Special	05-Apr-22	7.2	SQL Injection in ImpressCMS 1.4.3 and earlier allows remote attackers to inject	N/A	A-IMP-IMPR-190422/195

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			into the code in unintended way, this allows an attacker to read and modify the sensitive information from the database used by the application. If misconfigured, an attacker can even upload a malicious web shell to compromise the entire system. **CVE ID : CVE-2022-26986**		
Vendor: insights_from_google_pagespeed_project					
Product: insights_from_google_pagespeed					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	6.1	The Insights from Google PageSpeed WordPress plugin before 4.0.4 does not sanitise and escape various parameters before outputting them back in attributes in the plugin's settings dashboard, leading to Reflected Cross-Site Scripting **CVE ID : CVE-2022-0431**	https://plugins.trac.wordpress.org/changeset/2690415	A-INS-INSI-190422/196
Vendor: insurance_management_system_project					
Product: insurance_management_system					
Improper Neutralization of Special Elements used in an	05-Apr-22	9.8	Insurance Management System 1.0 was discovered to contain a SQL injection vulnerability	N/A	A-INS-INSU-190422/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			via the username parameter. **CVE ID : CVE-2022-27124**		
Vendor: ivanti					
Product: dsm_remote					
Unquoted Search Path or Element	11-Apr-22	7.8	Ivanti DSM Remote <= 6.3.1.1862 is vulnerable to an unquoted service path allowing local users to launch processes with elevated privileges. **CVE ID : CVE-2022-27088**	N/A	A-IVA-DSM_-190422/198
Product: incapptic_connect					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-22	4.8	An authenticated high privileged user can perform a stored XSS attack due to incorrect output encoding in Incapptic connect and affects all current versions. **CVE ID : CVE-2022-22571**	https://forums.ivanti.com/s/article/Security-Advisory-for-incapptic-Connect-SA-2022-03-11?language=en_US	A-IVA-INCA-190422/199
Vendor: jellycms					
Product: jellycms					
Unrestricted Upload of File with Dangerous Type	05-Apr-22	8.8	Jellycms v3.8.1 and below was discovered to contain an arbitrary file upload vulnerability via \app.\admin\Controllers\db.php. **CVE ID : CVE-2022-26630**	N/A	A-JEL-JELL-190422/200
Vendor: Jetbrains					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ktor					
Use of Insufficiently Random Values	11-Apr-22	2.7	In JetBrains Ktor Native before version 2.0.0 random values used for nonce generation weren't using SecureRandom implementations **CVE ID : CVE-2022-29035**	https://github.com/ktorio/ktor/pull/2776, https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-KTOR-190422/201
Vendor: jflyfox					
Product: jfinal_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-22	5.4	Jfinal_CMS 5.1.0 allows attackers to use the feedback function to send malicious XSS code to the administrator backend and execute it. **CVE ID : CVE-2022-27111**	N/A	A-JFL-JFIN-190422/202
Vendor: Kaspersky					
Product: anti-virus					
N/A	01-Apr-22	9.8	Kaspersky Anti-Virus products for home and Kaspersky Endpoint Security with antivirus databases released before 12 March 2022 had a bug in a data parsing module that potentially allowed an attacker to execute arbitrary code. The fix was delivered automatically. Credits: Georgy Zaytsev (Positive Technologies).	N/A	A-KAS-ANTI-190422/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-27534		
Product: endpoint_security					
N/A	01-Apr-22	9.8	Kaspersky Anti-Virus products for home and Kaspersky Endpoint Security with antivirus databases released before 12 March 2022 had a bug in a data parsing module that potentially allowed an attacker to execute arbitrary code. The fix was delivered automatically. Credits: Georgy Zaytsev (Positive Technologies). **CVE ID : CVE-2022-27534**	N/A	A-KAS-ENDP-190422/204
Product: internet_security					
N/A	01-Apr-22	9.8	Kaspersky Anti-Virus products for home and Kaspersky Endpoint Security with antivirus databases released before 12 March 2022 had a bug in a data parsing module that potentially allowed an attacker to execute arbitrary code. The fix was delivered automatically. Credits: Georgy Zaytsev (Positive Technologies). **CVE ID : CVE-2022-27534**	N/A	A-KAS-INTE-190422/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: security_cloud					
N/A	01-Apr-22	9.8	Kaspersky Anti-Virus products for home and Kaspersky Endpoint Security with antivirus databases released before 12 March 2022 had a bug in a data parsing module that potentially allowed an attacker to execute arbitrary code. The fix was delivered automatically. Credits: Georgy Zaytsev (Positive Technologies). **CVE ID : CVE-2022-27534**	N/A	A-KAS-SECU-190422/206
Product: small_office_security					
N/A	01-Apr-22	9.8	Kaspersky Anti-Virus products for home and Kaspersky Endpoint Security with antivirus databases released before 12 March 2022 had a bug in a data parsing module that potentially allowed an attacker to execute arbitrary code. The fix was delivered automatically. Credits: Georgy Zaytsev (Positive Technologies). **CVE ID : CVE-2022-27534**	N/A	A-KAS-SMAL-190422/207
Product: total_security					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Apr-22	9.8	Kaspersky Anti-Virus products for home and Kaspersky Endpoint Security with antivirus databases released before 12 March 2022 had a bug in a data parsing module that potentially allowed an attacker to execute arbitrary code. The fix was delivered automatically. Credits: Georgy Zaytsev (Positive Technologies). **CVE ID : CVE-2022-27534**	N/A	A-KAS-TOTA-190422/208
Vendor: kopano					
Product: groupware_core					
Improper Authentication	01-Apr-22	9.8	An issue in provider/libserver/ECKrbAuth.cpp of Kopano-Core v11.0.2.51 contains an issue which allows attackers to authenticate even if the user account or password is expired. **CVE ID : CVE-2022-26562**	https://stash.kopano.io/projects/KC/repos/kopanocore/browse/provider/libserver/ECKrbAuth.cpp#137, https://kopano.com/	A-KOP-GROU-190422/209
Vendor: Kyocera					
Product: net_viewer					
Insufficiently Protected Credentials	04-Apr-22	8.6	Kyocera multifunction printers running vulnerable versions of Net View unintentionally	https://www.kyoceradocumentsolutions.com/en/our-business/security/informatio	A-KYO-NET_-190422/210

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			expose sensitive user information, including usernames and passwords, through an insufficiently protected address book export function. **CVE ID : CVE-2022-1026**	n/2022-04-04.html	
Vendor: libsixel_project					
Product: libsixel					
Out-of-bounds Write	08-Apr-22	8.8	libsixel 1.8.6 is affected by Buffer Overflow in libsixel/src/quant.c:876. **CVE ID : CVE-2022-27044**	N/A	A-LIB-LIBS-190422/211
Use After Free	08-Apr-22	8.8	libsixel 1.8.6 suffers from a Heap Use After Free vulnerability in in libsixel/src/dither.c:388. **CVE ID : CVE-2022-27046**	N/A	A-LIB-LIBS-190422/212
Vendor: Libtiff					
Product: libtiff					
Uncontrolled Resource Consumption	03-Apr-22	6.5	A vulnerability classified as problematic was found in LibTIFF 4.3.0. Affected by this vulnerability is the TIFF File Handler of tiff2ps. Opening a malicious file leads to a denial of service. The attack can be launched remotely	N/A	A-LIB-LIBT-190422/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			but requires user interaction. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2022-1210**		
Vendor: Linux					
Product: linux_kernel					
N/A	02-Apr-22	7.5	In the Linux kernel before 5.17.1, a refcount leak bug was found in net/llc/af_llc.c. **CVE ID : CVE-2022-28356**	https://github.com/torvalds/linux/commit/764f4eb6846f5475f1244767d24d25dd86528a4a, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.17.1	A-LIN-LINU-190422/214
Vendor: livehelperchat					
Product: live_helper_chat					
Improper Encoding or Escaping of Output	07-Apr-22	8.8	Host Header injection in password Reset in GitHub repository livehelperchat/livehelperchat prior to 3.97. **CVE ID : CVE-2022-0935**	https://huntr.dev/bounties/a7e40fdf-a333-4a50-8a53-d11b16ce3ec2, https://github.com/livehelperchat/livehelperchat/commit/ce96791cb4c7420266b668fc234c211914259ba7	A-LIV-LIVE-190422/215
Server-Side Request	05-Apr-22	8.1	SSRF filter bypass port 80, 433 in GitHub repository livehelperchat/livehel	https://github.com/livehelperchat/livehelperchat/commit/	A-LIV-LIVE-190422/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			perchat prior to 3.67v. An attacker could make the application perform arbitrary requests, bypass CVE-2022-1191 **CVE ID : CVE-2022-1213**	abc9599ee7aded466ca216741dcaea533c908111, https://huntr.dev/bounties/084387f6-5b9c-4017-baa2-5fcf65b051e1	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-22	6.1	XSS in livehelperchat in GitHub repository livehelperchat/livehelperchat prior to 3.97. This vulnerability has the potential to deface websites, result in compromised user accounts, and can run malicious code on web pages, which can lead to a compromise of the userâ€™s device. **CVE ID : CVE-2022-1234**	https://github.com/livehelperchat/livehelperchat/commit/a09aa0d793818dc4cae78ac4bcfb557d4fd2a30d, https://huntr.dev/bounties/0d235252-0882-4053-85c1-b41b94c814d4	A-LIV-LIVE-190422/217
Use of Password Hash With Insufficient Computational Effort	05-Apr-22	8.2	Weak secrethash can be brute-forced in GitHub repository livehelperchat/livehelperchat prior to 3.96. **CVE ID : CVE-2022-1235**	https://github.com/livehelperchat/livehelperchat/commit/6538d6df3d8a60fee254170b08dd76a161f7bfdc, https://huntr.dev/bounties/92f7b2d4-fa88-4c62-a2ee-721eebe01705	A-LIV-LIVE-190422/218
Vendor: LUA					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: lua					
Out-of-bounds Read	08-Apr-22	9.1	singlevar in lparser.c in Lua through 5.4.4 lacks a certain luaK_exp2anyregup call, leading to a heap-based buffer over-read that might affect a system that compiles untrusted Lua code. **CVE ID : CVE-2022-28805**	https://github.com/lua/lua/commit/1f3c6f4534c6411313361697d98d1145a1f030fa	A-LUA-LUA-190422/219
Vendor: mappresspro					
Product: mappress_maps					
Unrestricted Upload of File with Dangerous Type	04-Apr-22	7.2	The MapPress Maps for WordPress plugin before 2.73.13 allows a high privileged user to bypass the DISALLOW_FILE_EDIT and DISALLOW_FILE_MODS settings and upload arbitrary files to the site through the "ajax_save" function. The file is written relative to the current 's stylesheet directory, and a .php file extension is added. No validation is performed on the content of the file, triggering an RCE vulnerability by uploading a web shell. Further the name parameter is not sanitized, allowing the payload to be	N/A	A-MAP-MAPP-190422/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uploaded to any directory to which the server has write access. **CVE ID : CVE-2022-0537**		
Vendor: mark_posts_project					
Product: mark_posts					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	4.8	The Mark Posts WordPress plugin before 2.0.1 does not escape new markers, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2022-0958**	https://plugins.trac.wordpress.org/changeset/2679436	A-MAR-MARK-190422/221
Vendor: material_design_for_contact_form_7_project					
Product: material_design_for_contact_form_7					
Incorrect Authorization	04-Apr-22	6.5	The Material Design for Contact Form 7 WordPress plugin through 2.6.4 does not check authorization or that the option mentioned in the notice param belongs to the plugin when processing requests to the cf7md_dismiss_notice action, allowing any logged in user (with roles as low as Subscriber) to set arbitrary options to	N/A	A-MAT-MATE-190422/222

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			true, potentially leading to Denial of Service by breaking the site. **CVE ID : CVE-2022-0404**		
Vendor: matrimony_project					
Product: matrimony					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-22	9.8	Matrimony v1.0 was discovered to contain a SQL injection vulnerability via the Password parameter. **CVE ID : CVE-2022-26628**	N/A	A-MAT-MATR-190422/223
Vendor: Microsoft					
Product: edge_chromium					
Improper Privilege Management	05-Apr-22	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-26891, CVE-2022-26894, CVE-2022-26895, CVE-2022-26900, CVE-2022-26908, CVE-2022-26909, CVE-2022-26912. **CVE ID : CVE-2022-24475**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24475	A-MIC-EDGE-190422/224
N/A	05-Apr-22	4.3	Microsoft Edge (Chromium-based) Spoofing Vulnerability. **CVE ID : CVE-2022-24523**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24523	A-MIC-EDGE-190422/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	05-Apr-22	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24475, CVE-2022-26894, CVE-2022-26895, CVE-2022-26900, CVE-2022-26908, CVE-2022-26909, CVE-2022-26912. **CVE ID : CVE-2022-26891**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26891	A-MIC-EDGE-190422/226
Improper Privilege Management	05-Apr-22	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24475, CVE-2022-26891, CVE-2022-26895, CVE-2022-26900, CVE-2022-26908, CVE-2022-26909, CVE-2022-26912. **CVE ID : CVE-2022-26894**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26894	A-MIC-EDGE-190422/227
Improper Privilege Management	05-Apr-22	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24475, CVE-2022-26891, CVE-2022-26894, CVE-2022-26900, CVE-2022-26908, CVE-2022-26909, CVE-2022-26912. **CVE ID : CVE-2022-26895**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26895	A-MIC-EDGE-190422/228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	05-Apr-22	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24475, CVE-2022-26891, CVE-2022-26894, CVE-2022-26895, CVE-2022-26908, CVE-2022-26909, CVE-2022-26912. **CVE ID : CVE-2022-26900**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26900	A-MIC-EDGE-190422/229
Improper Privilege Management	05-Apr-22	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24475, CVE-2022-26891, CVE-2022-26894, CVE-2022-26895, CVE-2022-26900, CVE-2022-26909, CVE-2022-26912. **CVE ID : CVE-2022-26908**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26908	A-MIC-EDGE-190422/230
Improper Privilege Management	05-Apr-22	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24475, CVE-2022-26891, CVE-2022-26894, CVE-2022-26895, CVE-2022-26900, CVE-2022-26908, CVE-2022-26912. **CVE ID : CVE-2022-26909**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26909	A-MIC-EDGE-190422/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	05-Apr-22	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24475, CVE-2022-26891, CVE-2022-26894, CVE-2022-26895, CVE-2022-26900, CVE-2022-26908, CVE-2022-26909. **CVE ID : CVE-2022-26912**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26912	A-MIC-EDGE-190422/232
Vendor: mingsoft					
Product: mcms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-22	9.8	Mingsoft MCMS v5.2.7 was discovered to contain a SQL injection vulnerability via /cms/content/list. **CVE ID : CVE-2022-26585**	N/A	A-MIN-MCMS-190422/233
Vendor: miraheze					
Product: createwiki					
Improper Authentication	04-Apr-22	5.3	CreateWiki is Miraheze's MediaWiki extension for requesting & creating wikis. Without the patch for this issue, anonymous comments can be made using Special:RequestWikiQueue when sent directly via POST. A patch for this issue is available in the	https://github.com/miraheze/CreateWiki/security/advisories/GHSA-9xvw-w66v-prvg, https://github.com/miraheze/CreateWiki/commit/d0ae79843d689832ccac765d6b1721e668d99ab9,	A-MIR-CREA-190422/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`master` branch of CreateWiki's GitHub repository. **CVE ID : CVE-2022-24813**	https://phabricator.miraheze.org/T9018	
Vendor: modbustools					
Product: modbus_slave					
Out-of-bounds Write	01-Apr-22	7.5	Modbus Tools Modbus Slave (versions 7.4.2 and prior) is vulnerable to a stack-based buffer overflow in the registration field. This may cause the program to crash when a long character string is used. **CVE ID : CVE-2022-1068**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-088-04	A-MOD-MODB-190422/235
Vendor: moguit					
Product: mogu_blog_cms					
Unrestricted Upload of File with Dangerous Type	08-Apr-22	9.8	mogu_blog_cms 5.2 suffers from upload arbitrary files without any limitation. **CVE ID : CVE-2022-27047**	N/A	A-MOG-MOGU-190422/236
Vendor: momentjs					
Product: moment					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Apr-22	7.5	Moment.js is a JavaScript date library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability impacts npm (server) users of Moment.js between	https://github.com/moment/moment/commit/4211bfc8f15746be4019bba557e29a7ba83d54c5, https://github.com/moment/moment/secur	A-MOM-MOME-190422/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 1.0.1 and 2.29.1, especially if a user-provided locale string is directly used to switch moment locale. This problem is patched in 2.29.2, and the patch can be applied to all affected versions. As a workaround, sanitize the user-provided locale name before passing it to Moment.js. **CVE ID : CVE-2022-24785**	ity/advisories/GHSA-8hfj-j24r-96c4	
Vendor: movie_seat_reservation_project					
Product: movie_seat_reservation					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Apr-22	9.8	Movie Seat Reservation v1 was discovered to contain a SQL injection vulnerability at /index.php?page=reserve via the id parameter. **CVE ID : CVE-2022-28001**	N/A	A-MOV-MOVI-190422/238
Files or Directories Accessible to External Parties	08-Apr-22	7.5	Movie Seat Reservation v1 was discovered to contain an unauthenticated file disclosure vulnerability via /index.php?page=home. **CVE ID : CVE-2022-28002**	N/A	A-MOV-MOVI-190422/239
Vendor: mruby					
Product: mruby					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	05-Apr-22	9.8	Use-After-Free in str_escape in mruby/mruby in GitHub repository mruby/mruby prior to 3.2. Possible arbitrary code execution if being exploited. **CVE ID : CVE-2022-1212**	https://github.com/mruby/mruby/commit/3cf291f72224715942beaf8553e42ba8891ab3c6, https://huntr.dev/bounties/9fcc06d0-08e4-49c8-afda-2cae40946abe	A-MRU-MRUB-190422/240
Out-of-bounds Read	10-Apr-22	9.8	Out-of-bounds Read in mrb_get_args in GitHub repository mruby/mruby prior to 3.2. Possible arbitrary code execution if being exploited. **CVE ID : CVE-2022-1276**	https://github.com/mruby/mruby/commit/c8c083cb750606b2da81582cd8e43b442bb143e6, https://huntr.dev/bounties/6ea041d1-e2aa-472c-bf3e-da5fa8726c25	A-MRU-MRUB-190422/241
Vendor: musical_world_project					
Product: musical_world					
Unrestricted Upload of File with Dangerous Type	08-Apr-22	8.8	Musical World v1 was discovered to contain an arbitrary file upload vulnerability via uploaded_songs.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-27064**	N/A	A-MUS-MUSI-190422/242
Vendor: Netflix					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: consoleme					
Use of Externally-Controlled Format String	01-Apr-22	9.8	A Python format string issue leading to information disclosure and potentially remote code execution in ConsoleMe for all versions prior to 1.2.2 **CVE ID : CVE-2022-27177**	N/A	A-NET-CONS-190422/243
Vendor: newbee-mall_project					
Product: newbee-mall					
Unrestricted Upload of File with Dangerous Type	10-Apr-22	9.8	Newbee-Mall v1.0.0 was discovered to contain an arbitrary file upload via the Upload function at /admin/goods/edit. **CVE ID : CVE-2022-27477**	N/A	A-NEW-NEWB-190422/244
Vendor: nginxproxymanager					
Product: nginx_proxy_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Apr-22	4.8	jc21.com Nginx Proxy Manager before 2.9.17 allows XSS during item deletion. **CVE ID : CVE-2022-28379**	N/A	A-NGI-NGIN-190422/245
Vendor: nootheme					
Product: jobmonster					
Improper Limitation of a Pathname to a Restricted	04-Apr-22	5.3	The JobMonster Theme was vulnerable to Directory Listing in the /wp-content/uploads/job	N/A	A-NOO-JOBM-190422/246

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			monster/ folder, as it did not include a default PHP file, or .htaccess file. This could expose personal data such as people's resumes. Although Directory Listing can be prevented by securely configuring the web server, vendors can also take measures to make it less likely to happen. **CVE ID : CVE-2022-1166**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	6.1	In the Noo JobMonster WordPress theme before 4.5.2.9 JobMonster there is a XSS vulnerability as the input for the search form is provided through unsanitized GET requests. **CVE ID : CVE-2022-1170**	N/A	A-NOO-JOBM-190422/247
Vendor: nsthemes					
Product: ns_watermark_for_woocommerce					
N/A	11-Apr-22	7.5	An unprivileged user could use the functionality of the NS WooCommerce Watermark WordPress plugin through 2.11.3 to load images that hide malware for example from passing	N/A	A-NST-NS_W-190422/248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious domains to hide their trace, by making them pass through the vulnerable domain. **CVE ID : CVE-2022-0989**		
Vendor: ocdi					
Product: one_click_demo_import					
Unrestricted Upload of File with Dangerous Type	11-Apr-22	7.2	The One Click Demo Import WordPress plugin before 3.1.0 does not validate the imported file, allowing high privilege users such as admin to upload arbitrary files (such as PHP) even when FILE_MODS and FILE_EDIT are disallowed **CVE ID : CVE-2022-1008**	https://wpscan.com/vulnerability/0c2e2b4d-49eb-4fd9-b9f0-3feae80c1082, https://plugins.trac.wordpress.org/changeset/2695999	A-OCD-ONE_-190422/249
Vendor: ofcms_project					
Product: ofcms					
Incorrect Default Permissions	10-Apr-22	5.4	Insecure permissions configured in the user_id parameter at SysUserController.java of OFCMS v1.1.4 allows attackers to access and arbitrarily modify users' personal information. **CVE ID : CVE-2022-27960**	N/A	A-OFC-OFCM-190422/250
Improper Neutralization of Input	10-Apr-22	5.4	A cross-site scripting (XSS) vulnerability at /ofcms/company-c-47 in OFCMS v1.1.4	N/A	A-OFC-OFCM-190422/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Comment text box. **CVE ID : CVE-2022-27961**		
Vendor: Omron					
Product: cx-position					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Apr-22	7.8	Omron CX-Position (versions 2.5.3 and prior) is vulnerable to memory corruption while processing a specific project file, which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-25959**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-088-02	A-OMR-CX-P-190422/252
Out-of-bounds Write	01-Apr-22	7.8	Omron CX-Position (versions 2.5.3 and prior) is vulnerable to an out-of-bounds write while processing a specific project file, which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-26022**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-088-02	A-OMR-CX-P-190422/253
Use After Free	01-Apr-22	7.8	Omron CX-Position (versions 2.5.3 and prior) is vulnerable to a use after free memory condition while processing a specific project file, which may allow an	https://www.cisa.gov/uscert/ics/advisories/icsa-22-088-02	A-OMR-CX-P-190422/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code. **CVE ID : CVE-2022-26417**		
Out-of-bounds Write	01-Apr-22	7.8	Omron CX-Position (versions 2.5.3 and prior) is vulnerable to multiple stack-based buffer overflow conditions while parsing a specific project file, which may allow an attacker to locally execute arbitrary code. **CVE ID : CVE-2022-26419**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-088-02	A-OMR-CX-P-190422/255
Vendor: online_banking_system_project					
Product: online_banking_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Apr-22	6.5	Online Banking System in PHP v1 was discovered to contain multiple SQL injection vulnerabilities at /staff_login.php via the Staff ID and Staff Password parameters. **CVE ID : CVE-2022-27991**	N/A	A-ONL-ONLI-190422/256
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-22	9.8	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter. **CVE ID : CVE-2022-28116**	N/A	A-ONL-ONLI-190422/257
Vendor: online_car_rental_system_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: online_car_rental_system					
Unrestricted Upload of File with Dangerous Type	04-Apr-22	8.8	Car Rental System v1.0 contains an arbitrary file upload vulnerability via the Add Car component which allows attackers to upload a webshell and execute arbitrary code. **CVE ID : CVE-2022-28062**	N/A	A-ONL-ONLI-190422/258
Vendor: online_project_time_management_system_project					
Product: online_project_time_management_system					
Unrestricted Upload of File with Dangerous Type	07-Apr-22	8.8	Online Project Time Management System v1.0 was discovered to contain an arbitrary file write vulnerability which allows attackers to execute arbitrary code via a crafted HTML file. **CVE ID : CVE-2022-26627**	N/A	A-ONL-ONLI-190422/259
Vendor: online_sports_complex_booking_project					
Product: online_sports_complex_booking					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-22	9.8	Online Sports Complex Booking v1.0 was discovered to contain a SQL injection vulnerability via the id parameter. **CVE ID : CVE-2022-28115**	N/A	A-ONL-ONLI-190422/260
Vendor: online_student_admission_project					
Product: online_student_admission					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-22	9.8	Online Student Admission v1.0 was discovered to contain a SQL injection vulnerability via the txtapplicationID parameter. **CVE ID : CVE-2022-28467**	N/A	A-ONL-ONLI-190422/261
Vendor: onlyoffice					
Product: document_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Apr-22	6.1	A cross-site scripting (XSS) vulnerability in ONLYOFFICE Document Server Example before v7.0.0 allows remote attackers inject arbitrary HTML or JavaScript through /example/editor. **CVE ID : CVE-2022-24229**	N/A	A-ONL-DOCU-190422/262
Vendor: Orangehrm					
Product: orangehrm					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-22	5.4	OrangeHRM 4.10 is vulnerable to Stored XSS in the "Share Video" section under "OrangeBuzz" via the GET/POST "createVideo[linkAddress]" parameter **CVE ID : CVE-2022-27107**	N/A	A-ORA-ORAN-190422/263
Authorization Bypass Through User-	06-Apr-22	4.3	OrangeHRM 4.10 is vulnerable to Insecure Direct Object Reference (IDOR) via the end point	N/A	A-ORA-ORAN-190422/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Key			symfony/web/index.php/time/createTimesheet`. Any user can create a timesheet in another user's account. **CVE ID : CVE-2022-27108**		
URL Redirection to Untrusted Site ('Open Redirect')	06-Apr-22	5.4	OrangeHRM 4.10 suffers from a Referer header injection redirect vulnerability. **CVE ID : CVE-2022-27109**	N/A	A-ORA-ORAN-190422/265
URL Redirection to Untrusted Site ('Open Redirect')	06-Apr-22	5.4	OrangeHRM 4.10 is vulnerable to a Host header injection redirect via viewPersonalDetails endpoint. **CVE ID : CVE-2022-27110**	N/A	A-ORA-ORAN-190422/266
Vendor: os4ed					
Product: opensis					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Apr-22	7.5	Due to lack of protection, parameter student_id in OpenSIS Classic 8.0 /modules/eligibility/Student.php can be used to inject SQL queries to extract information from databases. **CVE ID : CVE-2022-27041**	https://github.com/OS4ED/openSIS-Classic/issues/248	A-OS4-OPEN-190422/267
Vendor: Owncloud					
Product: owncloud					
N/A	07-Apr-22	6.8	ownCloud owncloud/android	https://owncloud.com/securit	A-OWN-OWNC-190422/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 2.20 has Incorrect Access Control for physically proximate attackers. **CVE ID : CVE-2022-25338**	y-advisories/cve-2022-25338/	
N/A	07-Apr-22	5.5	ownCloud owncloud/android 2.20 has Incorrect Access Control for local attackers. **CVE ID : CVE-2022-25339**	https://owncloud.com/security-advisories/cve-2022-25339/	A-OWN-OWNC-190422/269
Vendor: payroll_management_system_project					
Product: payroll_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-22	9.8	Payroll Management System v1.0 was discovered to contain a SQL injection vulnerability via the username parameter. **CVE ID : CVE-2022-28468**	N/A	A-PAY-PAYR-190422/270
Vendor: php-cms_project					
Product: php-cms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Apr-22	9.8	PHP-CMS v1.0 was discovered to contain a SQL injection vulnerability via the category parameter in categorymenu.php. **CVE ID : CVE-2022-26613**	N/A	A-PHP-PHP--190422/271
Vendor: Phpipam					
Product: phpipam					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	04-Apr-22	6.5	Improper Access Control in GitHub repository phpipam/phpipam prior to 1.4.6. **CVE ID : CVE-2022-1223**	https://huntr.dev/bounties/baec4c23-2466-4b13-b3c0-eaf1d000d4ab, https://github.com/phpipam/phpipam/commit/f6a49fd9f93b7d7e0a4fbf1d35338502eed35953	A-PHP-PHPI-190422/272
Incorrect Authorization	04-Apr-22	6.5	Improper Authorization in GitHub repository phpipam/phpipam prior to 1.4.6. **CVE ID : CVE-2022-1224**	https://github.com/phpipam/phpipam/commit/f6a49fd9f93b7d7e0a4fbf1d35338502eed35953, https://huntr.dev/bounties/cd9e1508-5682-427e-a921-14b4f520b85a	A-PHP-PHPI-190422/273
Incorrect Privilege Assignment	04-Apr-22	6.5	Incorrect Privilege Assignment in GitHub repository phpipam/phpipam prior to 1.4.6. **CVE ID : CVE-2022-1225**	https://github.com/phpipam/phpipam/commit/f6a49fd9f93b7d7e0a4fbf1d35338502eed35953, https://huntr.dev/bounties/49b44cfa-d142-4d79-b529-7805507169d2	A-PHP-PHPI-190422/274
Vendor: pickplugins					
Product: post_grid					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-22	6.4	The Post Grid WordPress plugin before 2.1.16 does not sanitise and escape the post_types parameter before outputting it back in the response of the post_grid_update_taxonomies_terms_by_posttypes AJAX action, available to any authenticated users, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-0447**	N/A	A-PIC-POST-190422/275
Vendor: Pimcore					
Product: pimcore					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Apr-22	7.5	SQL injection in RecyclebinController.php in GitHub repository pimcore/pimcore prior to 10.3.5. This vulnerability is capable of steal the data **CVE ID : CVE-2022-1219**	https://github.com/pimcore/pimcore/commit/a697830359df06246acca502ee2455614de68017, https://huntr.dev/bounties/f700bd18-1fd3-4a05-867f-07176aebc7f6	A-PIM-PIMC-190422/276
Vendor: pivotal_software					
Product: spring_framework					
Allocation of Resources Without Limits or Throttling	01-Apr-22	6.5	n Spring Framework versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may	https://tanzu.vmware.com/security/cve-2022-22950	A-PIV-SPRI-190422/277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service condition. **CVE ID : CVE-2022-22950**		
Vendor: pjsip					
Product: pjsip					
Out-of-bounds Read	06-Apr-22	9.8	PJSIP is a free and open source multimedia communication library written in C. PJSIP versions 2.12 and prior do not parse incoming RTCP feedback RPSI (Reference Picture Selection Indication) packet, but any app that directly uses pjmedia_rtcp_fb_parse_rpsi() will be affected. A patch is available in the `master` branch of the `pjsip/pjproject` GitHub repository. There are currently no known workarounds. **CVE ID : CVE-2022-24786**	https://github.com/pjsip/pjproject/security/advisories/GHSA-vhxv-phmx-g52q, https://github.com/pjsip/pjproject/commit/11559e49e65bdf00922ad5ae28913ec6a198d508	A-PJS-PJSI-190422/278
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Apr-22	7.5	PJSIP is a free and open source multimedia communication library written in C. A buffer overflow vulnerability in versions 2.12 and prior affects applications that uses PJSIP DNS resolution.	https://github.com/pjsip/pjproject/commit/9fae8f43accef8ea65d4a8ae9cdf297c46cfe29a, https://github.com/pjsip/pjproject/security/advisories/G	A-PJS-PJSI-190422/279

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It doesn't affect PJSIP users who utilize an external resolver. A patch is available in the \`master\` branch of the \`pjsip/pjproject\` GitHub repository. A workaround is to disable DNS resolution in PJSIP config (by setting \`nameserver_count\` to zero) or use an external resolver instead. **CVE ID : CVE-2022-24793**	HSA-p6g5-v97c-w5q4	
Vendor: plugin-planet					
Product: blackhole_for_bad_bots					
Authorization Bypass Through User-Controlled Key	04-Apr-22	9.1	The Blackhole for Bad Bots WordPress plugin before 3.3.2 uses headers such as CF-CONNECTING-IP, CLIENT-IP etc to determine the IP address of requests hitting the blackhole URL, which allows them to be spoofed. This could result in blocking arbitrary IP addresses, such as legitimate/good search engine crawlers / bots. This could also be abused by competitors to cause damage related to visibility in search engines, can be used to bypass arbitrary blocks caused by this	https://plugins.trac.wordpress.org/changeset/2666486	A-PLU-BLAC-190422/280

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plugin, block any visitor or even the administrator and even more. **CVE ID : CVE-2022-1165**		
Vendor: podman_project					
Product: podman					
Incorrect Default Permissions	04-Apr-22	7.5	A flaw was found in Podman, where containers were started incorrectly with non-empty default permissions. A vulnerability was found in Moby (Docker Engine), where containers were started incorrectly with non-empty inheritable Linux process capabilities. This flaw allows an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs. **CVE ID : CVE-2022-27649**	https://github.com/containers/podman/commit/aafa80918a245edcbdaceb1191d749570f1872d0	A-POD-PODM-190422/281
Vendor: pootlepress					
Product: easy_smooth_scroll_links					
Improper Neutralization of Input During Web Page	11-Apr-22	4.8	The Easy Smooth Scroll Links WordPress plugin before 2.23.1 does not sanitise and escape its settings, which could	N/A	A-POO-EASY-190422/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			allow high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2022-0728**		
Vendor: presscustomizr					
Product: nimble_page_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-22	6.1	The Nimble Page Builder WordPress plugin before 3.2.2 does not sanitise and escape the preview-level-guid parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-0314**	N/A	A-PRE-NIMB-190422/283
Vendor: program					
Product: parking_lot_management_system					
N/A	07-Apr-22	5.3	Microprogram's parking lot management system is vulnerable to sensitive information exposure. An unauthorized remote attacker can input specific URLs to acquire partial system configuration information. **CVE ID : CVE-2022-25594**	N/A	A-PRO-PARK-190422/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: public_knowledge_project					
Product: open_journal_systems					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Apr-22	6.1	Cross-site scripting (XSS) via Host Header injection in PKP Open Journals System 2.4.8 >= 3.3 allows remote attackers to inject arbitary code via the X-Forwarded-Host Header. **CVE ID : CVE-2022-24181**	N/A	A-PUB-OPEN-190422/285
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	6.1	PKP Vendor Open Journal System v2.4.8 to v3.3.8 allows attackers to perform reflected cross-site scripting (XSS) attacks via crafted HTTP headers. **CVE ID : CVE-2022-26616**	https://forum.pkp.sfu.ca/t/ojs-omp-ops-3-3-0-9-released/72236	A-PUB-OPEN-190422/286
Vendor: Qdpm					
Product: qdpm					
Cross-Site Request Forgery (CSRF)	08-Apr-22	8.8	qdPM 9.2 allows Cross-Site Request Forgery (CSRF) via the index.php/myAccount/update URI. **CVE ID : CVE-2022-26180**	N/A	A-QDP-QDPM-190422/287
Vendor: Radare					
Product: radare2					
Out-of-bounds Read	01-Apr-22	6.6	Out-of-bounds read in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability allows	https://github.com/radareorg/radare2/commit/605785b65dd356d46d4	A-RAD-RADA-190422/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to read sensitive information from outside the allocated buffer boundary. **CVE ID : CVE-2022-1207**	487faa41dbf90943b8bc1, https://huntr.dev/bounties/7b979e76-ae54-4132-b455-0833e45195eb	
Improper Validation of Array Index	06-Apr-22	7.8	Improper Validation of Array Index in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability is heap overflow and may be exploitable. For more general description of heap buffer overflow, see [CWE](https://cwe.mitre.org/data/definitions/122.html). **CVE ID : CVE-2022-1237**	https://huntr.dev/bounties/ad3c9c4c-76e7-40c8-bd4a-c095acd8bb40, https://github.com/radareorg/radare2/commit/2d782cdaa2112c10b8dd5e7a93c134b2ada9c1a6	A-RAD-RADA-190422/289
Buffer Access with Incorrect Length Value	06-Apr-22	7.8	Heap-based Buffer Overflow in libr/bin/format/ne/ne.c in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability is heap overflow and may be exploitable. For more general description of heap buffer overflow, see [CWE](https://cwe.mitre.org/data/definitions/122.html). **CVE ID : CVE-2022-1238**	https://github.com/radareorg/radare2/commit/c40a4f9862104ede15d0ba05ccbf805923070778, https://huntr.dev/bounties/47422cdf-aad2-4405-a6a1-6f63a3a93200	A-RAD-RADA-190422/290

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-22	7.8	Heap buffer overflow in libr/bin/format/mach0/mach0.c in GitHub repository radareorg/radare2 prior to 5.8.6. If address sanitizer is disabled during the compiling, the program should executes into the `r_str_ncpy` function. Therefore I think it is very likely to be exploitable. For more general description of heap buffer overflow, see [CWE](https://cwe.mitre.org/data/definitions/122.html). **CVE ID : CVE-2022-1240**	https://huntr.dev/bounties/e589bd97-4c74-4e79-93b5-0951a281facc, https://github.com/radareorg/radare2/commit/ca8d8b39f3e34a4fd943270330b80f1148129de4	A-RAD-RADA-190422/291
Heap-based Buffer Overflow	05-Apr-22	5.5	heap-buffer-overflow in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability is capable of inducing denial of service. **CVE ID : CVE-2022-1244**	https://github.com/radareorg/radare2/commit/2b77b277d67ce061ee6ef839e7139ebc2103c1e3, https://huntr.dev/bounties/8ae2c61a-2220-47a5-bfe8-fe6d41ab1f82	A-RAD-RADA-190422/292
NULL Pointer Dereference	08-Apr-22	5.5	NULL Pointer Dereference in r_bin_ne_get_entrypoints function in GitHub repository radareorg/radare2	https://huntr.dev/bounties/bfeb8fb8-644d-4587-80d4-cb704c404013	A-RAD-RADA-190422/293

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 5.6.8. This vulnerability allows attackers to cause a denial of service (application crash). **CVE ID : CVE-2022-1283**	, https://github.com/radareorg/radare2/commit/18d1d064bf599a255d55f09fca3104776fc34a67	
Use After Free	08-Apr-22	5.5	heap-use-after-free in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability is capable of inducing denial of service. **CVE ID : CVE-2022-1284**	https://huntr.dev/bounties/e98ad92c-3a64-48fb-84d4-d13afdbcbdd7, https://github.com/radareorg/radare2/commit/64a82e284dddabaeb549228380103b57dead32a6	A-RAD-RADA-190422/294
Out-of-bounds Read	11-Apr-22	9.1	Out-of-bounds read in `r_bin_ne_get_relocs` function in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability may allow attackers to read sensitive information or cause a crash. **CVE ID : CVE-2022-1296**	https://huntr.dev/bounties/52b57274-0e1a-4d61-ab29-1373b555fea0, https://github.com/radareorg/radare2/commit/153bcdc29f11cd8c90e7d639a7405450f644ddb6	A-RAD-RADA-190422/295
Out-of-bounds Read	11-Apr-22	9.1	Out-of-bounds Read in r_bin_ne_get_entrypoints function in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability may allow attackers to	https://github.com/radareorg/radare2/commit/0a557045476a2969c7079aec9eeb29d02f2809c6, https://huntr.dev/bounties/	A-RAD-RADA-190422/296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟥	read sensitive information or cause a crash. **CVE ID : CVE-2022-1297**	ec538fa4-06c6-4050-a141-f60153ddeaac	
Vendor: rangerstudio					
Product: directus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	6.1	Directus is a real-time API and App dashboard for managing SQL database content. Prior to version 9.7.0, unauthorized JavaScript (JS) can be executed by inserting an iframe into the rich text html interface that links to a file uploaded HTML file that loads another uploaded JS file in its script tag. This satisfies the regular content security policy header, which in turn allows the file to run any arbitrary JS. This issue was resolved in version 9.7.0. As a workaround, disable the live embed in the what-you-see-is-what-you-get by adding `{ "media_live_embeds": false }` to the _Options Overrides_ option of the Rich Text HTML interface.	https://github.com/directus/directus/security/advisories/GHSA-xmjj-3c76-5w84, https://github.com/directus/directus/pull/12020	A-RAN-DIRE-190422/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24814		
Vendor: rc-httpd_project					
Product: rc-httpd					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Apr-22	7.5	The rc-httpd component through 2022-03-31 for 9front (Plan 9 fork) allows ..%2f directory traversal if serve-static is used. **CVE ID : CVE-2022-28380**	https://git.9front.org/plan9front/plan9front/241667b933ff5bacb9a3974f6877fb8aad78bed3/commit.html	A-RC--RC-H-190422/298
Vendor: realfavicongenerator					
Product: favicon_by_realfavicongenerator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-22	6.1	The Favicon by RealFaviconGenerator WordPress plugin before 1.3.23 does not properly sanitise and escape the json_result_url parameter before outputting it back in the Favicon admin dashboard, leading to a Reflected Cross-Site Scripting issue **CVE ID : CVE-2022-0471**	https://wpscan.com/vulnerability/499bfee4-b481-4276-b6ad-0eead6680f66, https://plugins.trac.wordpress.org/changeset/2695862	A-REA-FAVI-190422/299
Vendor: Redhat					
Product: openshift_container_platform					
Incorrect Default Permissions	04-Apr-22	7.5	A flaw was found in Podman, where containers were started incorrectly with non-empty default permissions. A vulnerability was found in Moby	https://github.com/containers/podman/commit/aafa80918a245edcbdaceb1191d749570f1872d0	A-RED-OPEN-190422/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Docker Engine), where containers were started incorrectly with non-empty inheritable Linux process capabilities. This flaw allows an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs. **CVE ID : CVE-2022-27649**		
Incorrect Default Permissions	04-Apr-22	7.5	A flaw was found in crun where containers were incorrectly started with non-empty default permissions. A vulnerability was found in Moby (Docker Engine) where containers were started incorrectly with non-empty inheritable Linux process capabilities. This flaw allows an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs. **CVE ID : CVE-2022-27650**	https://github.com/containers/crun/commit/1aeeed2e4fdeffb4875c0d0b439915894594c8c6	A-RED-OPEN-190422/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: reprisesoftware					
Product: reprise_license_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Apr-22	6.1	Reprise License Manager 14.2 is affected by a reflected cross-site scripting vulnerability (XSS) in the /goform/login_process username parameter via GET. No authentication is required. **CVE ID : CVE-2022-28363**	N/A	A-REP-REPR-190422/302
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Apr-22	5.4	Reprise License Manager 14.2 is affected by a reflected cross-site scripting vulnerability (XSS) in the /goform/rlmswitchr_process file parameter via GET. Authentication is required. **CVE ID : CVE-2022-28364**	N/A	A-REP-REPR-190422/303
Exposure of Resource to Wrong Sphere	09-Apr-22	5.3	Reprise License Manager 14.2 is affected by an Information Disclosure vulnerability via a GET request to /goforms/rlminfo. No authentication is required. The information disclosed is associated with software versions, process IDs, network	N/A	A-REP-REPR-190422/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration, hostname(s), system architecture, and file/directory details. **CVE ID : CVE-2022-28365**		
Vendor: rocket.chat					
Product: livechat					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Apr-22	6.1	A blind self XSS vulnerability exists in RocketChat LiveChat <v1.9 that could allow an attacker to trick a victim pasting malicious code in their chat instance. **CVE ID : CVE-2022-21830**	N/A	A-ROC-LIVE-190422/305
Vendor: Rockwellautomation					
Product: connected_components_workbench					
Improper Restriction of XML External Entity Reference	01-Apr-22	5.5	When opening a malicious solution file provided by an attacker, the application suffers from an XML external entity vulnerability due to an unsafe call within a dynamic link library file. An attacker could exploit this to pass data from local files to a remote web server, leading to a loss of confidentiality. **CVE ID : CVE-2022-1018**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-088-01	A-ROC-CONN-190422/306
Product: isagraf					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of XML External Entity Reference	01-Apr-22	5.5	When opening a malicious solution file provided by an attacker, the application suffers from an XML external entity vulnerability due to an unsafe call within a dynamic link library file. An attacker could exploit this to pass data from local files to a remote web server, leading to a loss of confidentiality. **CVE ID : CVE-2022-1018**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-088-01	A-ROC-ISAG-190422/307
Vendor: saasproject					
Product: booking_package					
N/A	04-Apr-22	7.5	The Booking Package WordPress plugin before 1.5.29 requires a token for exporting the ical representation of it's booking calendar, but this token is returned in the json response to unauthenticated users performing a booking, leading to a sensitive data disclosure vulnerability. **CVE ID : CVE-2022-0709**	N/A	A-SAA-BOOK-190422/308
Vendor: salonbookingsystem					
Product: salon_booking_system					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Apr-22	5.3	The Salon booking system Free and pro WordPress plugins before 7.6.3 do not have proper authorisation when searching bookings, allowing any unauthenticated users to search other's booking, as well as retrieve sensitive information about the bookings, such as the full name, email and phone number of the person who booked it. **CVE ID : CVE-2022-0919**	N/A	A-SAL-SALO-190422/309
Incorrect Authorization	11-Apr-22	7.5	The Salon booking system Free and Pro WordPress plugins before 7.6.3 do not have proper authorisation in some of its endpoints, which could allow customers to access all bookings and other customer's data **CVE ID : CVE-2022-0920**	N/A	A-SAL-SALO-190422/310
Vendor: sap_information_system_project					
Product: sap_information_system					
Improper Authentication	06-Apr-22	7.3	A vulnerability was found in SAP Information System 1.0 which has been rated as critical. Affected by this issue is the file	N/A	A-SAP-SAP_-190422/311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/SAP_Information_System/controllers/add_admin.php. An unauthenticated attacker is able to create a new admin account for the web application with a simple POST request. Exploit details were disclosed. **CVE ID : CVE-2022-1248**		
Vendor: scala-js					
Product: scala.js					
Use of Insufficiently Random Values	02-Apr-22	7.5	randomUUID in Scala.js before 1.10.0 generates predictable values. **CVE ID : CVE-2022-28355**	https://github.com/scala-js/scala-js/issues/4657 , https://www.scala-js.org/news/2022/04/04/announcing-scalajs-1.10.0/, https://github.com/scala-js/scala-js/security/advisories/GHSA-j2f9-w8wh-9ww4	A-SCA-SCAL-190422/312
Vendor: school_club_application_system_project					
Product: school_club_application_system					
Improper Neutralization of Special Elements in Output Used by a	09-Apr-22	9.8	A vulnerability classified as critical was found in School Club Application System 1.0. This vulnerability affects a request to the file	N/A	A-SCH-SCHO-190422/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Downstream Component ('Injection')			/scas/classes/Users.php?f=save_user. The manipulation with a POST request leads to privilege escalation. The attack can be initiated remotely and does not require authentication. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2022-1287**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Apr-22	6.1	A vulnerability, which was classified as problematic, has been found in School Club Application System 1.0. This issue affects access to /scas/admin/. The manipulation of the parameter page with the input %22%3E%3Cimg%20src=x%20onerror=alert(1)%3E leads to a reflected cross site scripting. The attack may be initiated remotely and does not require any form of authentication. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2022-1288**	N/A	A-SCH-SCHO-190422/314
Vendor: secom					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dr.id_access_control					
Use of Hard-coded Credentials	07-Apr-22	7.3	Taiwan Secom Dr.ID Access Control system's login page has a hard-coded credential in the source code. An unauthenticated remote attacker can use the hard-coded credential to acquire partial system information and modify system setting to cause partial disrupt of service. **CVE ID : CVE-2022-26671**	N/A	A-SEC-DR.I-190422/315
Product: dr.id_attendance_system					
Use of Hard-coded Credentials	07-Apr-22	7.3	Taiwan Secom Dr.ID Access Control system's login page has a hard-coded credential in the source code. An unauthenticated remote attacker can use the hard-coded credential to acquire partial system information and modify system setting to cause partial disrupt of service. **CVE ID : CVE-2022-26671**	N/A	A-SEC-DR.I-190422/316
Vendor: secondlinethemes					
Product: podcast_importer_secondline					
Improper Neutralization of	11-Apr-22	7.2	The Podcast Importer SecondLine WordPress plugin	https://plugins.trac.wordpress.org/changese	A-SEC-PODC-190422/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			before 1.3.8 does not sanitise and properly escape some imported data, which could allow SQL injection attacks to be performed by imported a malicious podcast file **CVE ID : CVE-2022-1023**	t/2696254, https://wpscan.com/vulnerability/163069cd-98a8-4cfb-8b58-a6727a7d5c48	
Vendor: simple-git_project					
Product: simple-git					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Apr-22	9.8	The package simple-git before 3.5.0 are vulnerable to Command Injection due to an incomplete fix of [CVE-2022-24433](https://security.snyk.io/vuln/SNYK-JS-SIMPLEGIT-2421199) which only patches against the git fetch attack vector. A similar use of the --upload-pack feature of git is also supported for git clone, which the prior fix didn't cover. **CVE ID : CVE-2022-24066**	https://gist.github.com/lirantal/a930d902294b833514e821102316426b, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2434820, https://github.com/steveukx/git-js/commit/2040de601c894363050fef9f28af367b169a56c5, https://snyk.io/vuln/SNYK-JS-SIMPLEGIT-2434306	A-SIM-SIMP-190422/318
Vendor: Simplemachines					
Product: simple_machines_forum					
Incorrect Permission Assignment for	05-Apr-22	7.2	SimpleMachinesForum 2.1.1 and earlier allows remote authenticated administrators to	N/A	A-SIM-SIMP-190422/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			execute arbitrary code by inserting a vulnerable php code because the themes can be modified by an administrator. **CVE ID : CVE-2022-26982**		
Vendor: simple_bakery_shop_management_system_project					
Product: simple_bakery_shop_management_system					
N/A	04-Apr-22	4.9	Simple Bakery Shop Management System v1.0 contains a file disclosure via /bsms/?page=products. **CVE ID : CVE-2022-28063**	N/A	A-SIM-SIMP-190422/320
Vendor: simple_house_rental_system_project					
Product: simple_house_rental_system					
Unrestricted Upload of File with Dangerous Type	08-Apr-22	8.8	Simple House Rental System v1 was discovered to contain an arbitrary file upload vulnerability via /app/register.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-27352**	N/A	A-SIM-SIMP-190422/321
Vendor: simple_student_information_system_project					
Product: simple_student_information_system					
Improper Neutralization of Input During	05-Apr-22	6.1	Simple Student Information System v1.0 was discovered to contain a SQL	N/A	A-SIM-SIMP-190422/322

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			injection vulnerability via add/Student. **CVE ID : CVE-2022-24231**		
Vendor: socialcodia					
Product: social_codia_sms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Apr-22	4.8	Social Codia SMS v1 was discovered to contain a stored cross-site scripting (XSS) vulnerability via add_post.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Post Title text field. **CVE ID : CVE-2022-27348**	N/A	A-SOC-SOCI-190422/323
Unrestricted Upload of File with Dangerous Type	08-Apr-22	7.2	Social Codia SMS v1 was discovered to contain an arbitrary file upload vulnerability via addteacher.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-27349**	N/A	A-SOC-SOCI-190422/324
Vendor: std42					
Product: elfinder					
Unrestricted Upload of File with Dangerous Type	11-Apr-22	9.8	In Studio-42 elFinder 2.1.60, there is a vulnerability that causes remote code execution through file	https://github.com/Studio-42/elFinder/issues/3458	A-STD-ELFI-190422/325

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			name bypass for file upload. **CVE ID : CVE-2022-27115**		
Vendor: stopbadbots					
Product: block_and_stop_bad_bots					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Apr-22	9.8	The Block Bad Bots and Stop Bad Bots Crawlers and Spiders and Anti Spam Protection WordPress plugin before 6.930 does not properly sanitise and escape the fingerprint parameter before using it in a SQL statement via the stopbadbots_grava_fingerprint AJAX action, available to unauthenticated users, leading to a SQL injection **CVE ID : CVE-2022-0949**	N/A	A-STO-BLOC-190422/326
Vendor: struktur					
Product: libde265					
Out-of-bounds Write	06-Apr-22	9.8	Heap-based Buffer Overflow in GitHub repository strukturag/libde265 prior to and including 1.0.8. The fix is established in commit 8e89fe0e175d2870c39486fdd09250b230ec10b8 but does not yet belong to an official release.	https://huntr.dev/bounties/1-other-strukturag/libde265, https://github.com/strukturag/libde265/commit/8e89fe0e175d2870c39486fdd09250b230ec10b8	A-STR-LIBD-190422/327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1253		
Vendor: student_grading_system_project					
Product: student_grading_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-22	9.8	Student Grading System v1.0 was discovered to contain a SQL injection vulnerability via the user parameter. **CVE ID : CVE-2022-27304**	N/A	A-STU-STUD-190422/328
Vendor: Suse					
Product: rancher_desktop					
Improper Access Control	01-Apr-22	8.8	A Improper Access Control vulnerability in Rancher Desktop of SUSE allows attackers in the local network to connect to the Dashboard API (steve) to carry out arbitrary actions. This issue affects: SUSE Rancher Desktop versions prior to V. **CVE ID : CVE-2022-21947**	https://bugzilla.suse.com/show_bug.cgi?id=1197491	A-SUS-RANC-190422/329
Vendor: swayvm					
Product: swaylock					
N/A	03-Apr-22	9.1	swaylock before 1.6 allows attackers to trigger a crash and achieve unlocked access to a Wayland compositor. **CVE ID : CVE-2022-26530**	https://bugzilla.redhat.com/show_bug.cgi?id=2066596, https://github.com/swaywm/swaylock/commit/1d1c75b6	A-SWA-SWAY-190422/330

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				316d21933069a9d201f966d84099f6ca, https://github.com/swaywm/swaylock/pull/219	
Vendor: Synametrics					
Product: synaman					
Incorrect Permission Assignment for Critical Resource	06-Apr-22	7.8	Synaman v5.1 and below was discovered to contain weak file permissions which allows authenticated attackers to escalate privileges. **CVE ID : CVE-2022-26250**	http://synaman.com, http://synametrics.com	A-SYN-SYNA-190422/331
Improper Privilege Management	06-Apr-22	7.2	The HTTP interface of Synaman v5.1 and below was discovered to allow authenticated attackers to execute arbitrary code and escalate privileges. **CVE ID : CVE-2022-26251**	http://synaman.com, http://synametrics.com	A-SYN-SYNA-190422/332
Vendor: tableexport.jquery.plugin_project					
Product: tableexport.jquery.plugin					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-22	5.4	XSS vulnerability with default `onCellHtmlData` function in GitHub repository hhurz/tableexport.jquery.plugin prior to 1.25.0. Transmitting cookies to third-party servers. Sending data	https://huntr.dev/bounties/49a14371-6058-47dd-9801-ec38a7459fc5, https://github.com/hhurz/tableexport.jquery.plugin/commit/dcbaee23cf9	A-TAB-TABL-190422/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from secure sessions to third-party servers **CVE ID : CVE-2022-1291**	8328397a153e71556f75202988ec9	
Vendor: tastyigniter					
Product: tastyigniter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-22	5.4	Cross-site Scripting (XSS) - DOM in GitHub repository tastyigniter/tastyigniter prior to 3.3.0. **CVE ID : CVE-2022-0602**	https://github.com/tastyigniter/tastyigniter/commit/992d4ce6444805c3132e3635a01b6fd222063554, https://huntr.dev/bounties/615f1788-d474-4580-b0ef-5edd50274010	A-TAS-TAST-190422/334
Vendor: thedaylightstudio					
Product: fuel_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-22	5.4	Daylight Studio Fuel CMS 1.5.1 is vulnerable to HTML Injection. **CVE ID : CVE-2022-27156**	https://github.com/daylightstudio/FUEL-CMS/issues/593	A-THE-FUEL-190422/335
Vendor: thimpress					
Product: learnpress					
Improper Neutralization of Input During Web Page Generation	11-Apr-22	6.1	The LearnPress WordPress plugin before 4.1.6 does not sanitise and escape the lp-dismiss-notice before outputting it back via the lp_background_single	N/A	A-THI-LEAR-190422/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			_email AJAX action, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-0271**		
Vendor: tildearrow					
Product: furnace					
Out-of-bounds Write	03-Apr-22	6.5	A vulnerability classified as critical has been found in tildearrow Furnace dev73. This affects the FUR to VGM converter in console mode which causes stack-based overflows and crashes. It is possible to initiate the attack remotely but it requires user-interaction. A POC has been disclosed to the public and may be used. **CVE ID : CVE-2022-1211**	https://github.com/tildearrow/furnace/issues/325	A-TIL-FURN-190422/337
Vendor: tms-outsource					
Product: amelia					
Incorrect Authorization	04-Apr-22	5.4	The Amelia WordPress plugin before 1.0.49 does not have proper authorisation when managing appointments, allowing any customer to update other's booking status, as well as retrieve sensitive	https://plugins.trac.wordpress.org/changeset/2693545	A-TMS-AMEL-190422/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about the bookings, such as the full name and phone number of the person who booked it. **CVE ID : CVE-2022-0825**		
Incorrect Authorization	04-Apr-22	5.4	The Amelia WordPress plugin before 1.0.48 does not have proper authorisation when handling Amelia SMS service, allowing any customer to send paid test SMS notification as well as retrieve sensitive information about the admin, such as the email, account balance and payment history. A malicious actor can abuse this vulnerability to drain out the account balance by keep sending SMS notification. **CVE ID : CVE-2022-0837**	N/A	A-TMS-AMEL-190422/339
Product: wpdatatables_lite					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	4.8	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in wpDataTables (WordPress plugin) versions <= 2.1.27 **CVE ID : CVE-2022-25618**	https://wordpress.org/plugins/wpdatatables/#developers, https://patchstack.com/database/vulnerability/wpdatatables/wordpress-wpdatatables-plugin-2-1-27-	A-TMS-WPDA-190422/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				stored-cross-site-scripting-xss-vulnerability	
Vendor: totaljs					
Product: content_management_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Apr-22	4.8	A cross-site scripting (XSS) vulnerability in Totaljs commit 95f54a5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Page Name text field when creating a new page. **CVE ID : CVE-2022-26565**	https://github.com/totaljs/cms/issues/35	A-TOT-CONT-190422/341
Vendor: tpcms_project					
Product: tpcms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	4.8	A stored cross-site scripting (XSS) vulnerability in TPCMS v3.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Phone text box. **CVE ID : CVE-2022-27441**	N/A	A-TPC-TPCM-190422/342
Insertion of Sensitive Information into Log File	04-Apr-22	7.5	TPCMS v3.2 allows attackers to access the ThinkPHP log directory and obtain sensitive information such as the administrator's user name and password.	N/A	A-TPC-TPCM-190422/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-27442		
Vendor: Trendmicro					
Product: antivirus_for_mac					
Improper Link Resolution Before File Access ('Link Following')	09-Apr-22	7.3	A link following vulnerability in Trend Micro Antivirus for Mac 11.5 could allow an attacker to create a specially-crafted file as a symlink that can lead to privilege escalation. Please note that an attacker must at least have low-level privileges on the system to attempt to exploit this vulnerability. **CVE ID : CVE-2022-27883**	https://helpcenter.trendmicro.com/en-us/article/tmka-10978	A-TRE-ANTI-190422/344
Vendor: trudesk_project					
Product: trudesk					
Unrestricted Upload of File with Dangerous Type	11-Apr-22	5.4	Stored XSS viva .svg file upload in GitHub repository polonel/trudesk prior to v1.2.0. **CVE ID : CVE-2022-1045**	https://huntr.dev/bounties/b0c4f992-4ac8-4479-82f4-367ed1a2a826 , https://github.com/polonel/trudesk/commit/c4b262c2613d4a8865de0b3252112544bd81997a	A-TRU-TRUD-190422/345
Vendor: twistedmatrix					
Product: twisted					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Apr-22	8.1	Twisted is an event-based framework for internet applications, supporting Python 3.6+. Prior to version 22.4.0rc1, the Twisted Web HTTP 1.1 server, located in the `twisted.web.http` module, parsed several HTTP request constructs more leniently than permitted by RFC 7230. This non-conformant parsing can lead to desync if requests pass through multiple HTTP parsers, potentially resulting in HTTP request smuggling. Users who may be affected use Twisted Web's HTTP 1.1 server and/or proxy and also pass requests through a different HTTP server and/or proxy. The Twisted Web client is not affected. The HTTP 2.0 server uses a different parser, so it is not affected. The issue has been addressed in Twisted 22.4.0rc1. Two workarounds are available: Ensure any vulnerabilities in upstream proxies have been addressed, such as by upgrading	https://github.com/twisted/twisted/commit/592217e951363d60e9cd99c5bbfd23d4615043ac, https://github.com/twisted/twisted/security/advisories/GHSA-c2jg-hw38-jrqq	A-TWI-TWIS-190422/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			them; or filter malformed requests by other means, such as configuration of an upstream proxy. **CVE ID : CVE-2022-24801**		
Vendor: updraftplus					
Product: updraftplus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	6.1	The UpdraftPlus WordPress Backup Plugin WordPress plugin before 1.22.9 does not sanitise and escape the updraft_interval parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2022-0864**	N/A	A-UPD-UPDR-190422/347
Vendor: uri.js_project					
Product: uri.js					
Improper Input Validation	05-Apr-22	6.1	CRHTLF can lead to invalid protocol extraction potentially leading to XSS in GitHub repository medialize/uri.js prior to 1.19.11. **CVE ID : CVE-2022-1243**	https://huntr.dev/bounties/8c5afc47-1553-4eba-a98e-024e4cc3dfb7, https://github.com/medialize/uri.js/commit/b0c9796aa1a95a85f40924fb18b1e5da3dc8ffae	A-URI-URI.-190422/348
Vendor: url.js_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: url.js					
URL Redirection to Untrusted Site ('Open Redirect')	04-Apr-22	6.1	URL Confusion When Scheme Not Supplied in GitHub repository medialize/uri.js prior to 1.19.11. **CVE ID : CVE-2022-1233**	https://github.com/medialize/uri.js/commit/88805fd3da03bd7a5e60947adb49d182011f1277, https://huntr.dev/bounties/228d5548-1109-49f8-8aee-91038e88371c	A-URL-URL.-190422/349
Vendor: vcs_project					
Product: vcs					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	01-Apr-22	9.8	The package github.com/masterminds/vcs before 1.13.3 are vulnerable to Command Injection via argument injection. When hg is executed, argument strings are passed to hg in a way that additional flags can be set. The additional flags can be used to perform a command injection. **CVE ID : CVE-2022-21235**	https://github.com/Masterminds/vcs/pull/105	A-VCS-VCS-190422/350
Vendor: vertistudio					
Product: image_optimization_\&_lazy_load_by_optimole					
Improper Neutralization of Input During Web Page	11-Apr-22	4.8	The Image optimization & Lazy Load by Optimole WordPress plugin before 3.3.2 does not sanitise and escape its	https://plugins.trac.wordpress.org/changeset/2695242, https://wpscan.com/vulnera	A-VER-IMAG-190422/351

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			"Lazyload background images for selectors" settings, which could allow high privilege users such as admin to perform Cross-Site scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-0969**	bility/59a7a441-7384-4006-89b4-15345f70fabf	
Vendor: Vmware					
Product: spring_cloud_function					
Improper Control of Generation of Code ('Code Injection')	01-Apr-22	9.8	In Spring Cloud Function versions 3.1.6, 3.2.2 and older unsupported versions, when using routing functionality it is possible for a user to provide a specially crafted SpEL as a routing-expression that may result in remote code execution and access to local resources. **CVE ID : CVE-2022-22963**	https://tanzu.vmware.com/security/cve-2022-22963, https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0005	A-VMW-SPRI-190422/352
Product: spring_framework					
Improper Control of Generation of Code ('Code Injection')	01-Apr-22	9.8	A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the	https://tanzu.vmware.com/security/cve-2022-22965, https://psirt.global.sonicwall.com/vuln-	A-VMW-SPRI-190422/353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it. **CVE ID : CVE-2022-22965**	detail/SNWLID-2022-0005	
Vendor: vyper_project					
Product: vyper					
Incorrect Comparison	04-Apr-22	7.5	Vyper is a Pythonic Smart Contract Language for the Ethereum Virtual Machine. In version 0.3.1 and prior, bytestrings can have dirty bytes in them, resulting in the word-for-word comparisons giving incorrect results. Even without dirty nonzero bytes, two bytestrings can compare to equal if one ends with `"\x00"` because there is no comparison of the length. A patch is available and expected to be part of the 0.3.2 release. There are currently	https://github.com/vyperlang/vyper/commit/2c73f8352635c0a433423a5b94740de1a118e508, https://github.com/vyperlang/vyper/security/advisories/GHSA-7vrm-3jc8-5wwm	A-VYP-VYPE-190422/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			no known workarounds. **CVE ID : CVE-2022-24787**		
Vendor: waycrate					
Product: swhkd					
Exposure of Resource to Wrong Sphere	07-Apr-22	9.1	SWHKD 1.1.5 unsafely uses the /tmp/swhkd.sock pathname. There can be an information leak or denial of service. **CVE ID : CVE-2022-27818**	https://github.com/waycrate/swhkd/commit/f70b99dd575fab79d8a942111a6980431f006818, http://www.openwall.com/lists/oss-security/2022/04/14/1	A-WAY-SWHK-190422/355
Uncontrolled Resource Consumption	07-Apr-22	5.3	SWHKD 1.1.5 allows unsafe parsing via the -c option. An information leak might occur but there is a simple denial of service (memory exhaustion) upon an attempt to parse a large or infinite file (such as a block or character device). **CVE ID : CVE-2022-27819**	https://github.com/waycrate/swhkd/commit/b4e6dc76f4845ab03104187a42ac6d1bbc1e0021, http://www.openwall.com/lists/oss-security/2022/04/14/1	A-WAY-SWHK-190422/356
Vendor: webence					
Product: iq_block_country					
External Control of File Name or Path	11-Apr-22	4.9	The settings of the iQ Block Country WordPress plugin before 1.2.13 can be exported or imported using its backup functionality. An	N/A	A-WEB-IQ_B-190422/357

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authorized user can import preconfigured settings of the plugin by uploading a zip file. After the uploading process, files in the uploaded zip file are extracted one by one. During the extraction process, existence of a file is checked. If the file exists, it is deleted without any security control by only considering the name of the extracted file. This behavior leads to "Zip Slip" vulnerability. **CVE ID : CVE-2022-0246**		
Vendor: Weechat					
Product: weechat					
Improper Certificate Validation	02-Apr-22	4.8	WeeChat (aka Wee Enhanced Environment for Chat) 3.2 to 3.4 before 3.4.1 does not properly verify the TLS certificate of the server, after certain GnuTLS options are changed, which allows man-in-the-middle attackers to spoof a TLS chat server via an arbitrary certificate. NOTE: this only affects situations where weechat.network.gnu	https://weechat.org/doc/security/WSA-2022-1/	A-WEE-WEEC-190422/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tls_ca_system or weechat.network.gnu tls_ca_user is changed without a WeeChat restart. **CVE ID : CVE-2022-28352**		
Vendor: weseek					
Product: growi					
Weak Password Requirements	05-Apr-22	6.5	Weak Password Requirements in GitHub repository weseek/growi prior to v5.0.0. **CVE ID : CVE-2022-1236**	https://github.com/weseek/growi/commit/b584e2a47ee3c8ce1d8ef38238302825c015327e, https://huntr.dev/bounties/c7df088f-e355-45e6-9267-e41030dc6a32	A-WES-GROW-190422/359
Vendor: wisc					
Product: htcondor					
N/A	06-Apr-22	8.8	An issue was discovered in HTCondor 8.8.x before 8.8.16, 9.0.x before 9.0.10, and 9.1.x before 9.6.0. When a user authenticates to an HTCondor daemon via the CLAIMTOBE method, the user can then impersonate any entity when issuing additional commands to that daemon. **CVE ID : CVE-2022-26110**	N/A	A-WIS-HTCO-190422/360

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wpdownloadmanager					
Product: wordpress_download_manager					
Inadequate Encryption Strength	11-Apr-22	7.5	The Download Manager WordPress plugin before 3.2.39 uses the uniqid php function to generate the master key for a download, allowing an attacker to brute force the key with reasonable resources giving direct download access regardless of role based restrictions or password protections set for the download. **CVE ID : CVE-2022-0828**	N/A	A-WPD-WORD-190422/361
Vendor: wpjos					
Product: library_file_manager					
Unrestricted Upload of File with Dangerous Type	04-Apr-22	8.1	The Library File Manager WordPress plugin before 5.2.3 is using an outdated version of the elFinder library, which is know to be affected by security issues (CVE-2021-32682), and does not have any authorisation as well as CSRF checks in its connector AJAX action, allowing any authenticated users, such as subscriber to call it. Furthermore, as the options passed to the elFinder library	N/A	A-WPJ-LIBR-190422/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not restrict any file type, users with a role as low as subscriber can Create/Upload/Delete Arbitrary files and folders. **CVE ID : CVE-2022-0403**		
Vendor: wpvivid					
Product: migration\,_backup\,_staging					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-22	6.1	The Migration, Backup, Staging WordPress plugin before 0.9.70 does not sanitise and escape the sub_page parameter before outputting it back in the page, leading to a reflected Cross-Site Scripting **CVE ID : CVE-2022-0531**	N/A	A-WPV-MIGR-190422/363
Vendor: wwbn					
Product: avideo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-22	6.1	Cross Site Scripting (XSS) vulnerability in objects/function.php in function getDeviceID in WWBN AVideo through 11.6, via the yptDevice parameter to view/include/head.php. **CVE ID : CVE-2022-27462**	https://github.com/WWBN/AVideo/commit/3722335f808484e6bfb5e71028feddd942add4a	A-WWB-AVID-190422/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	05-Apr-22	6.1	Open redirect vulnerability in objects/login.json.php in WWBN AVideo through 11.6, allows attackers to arbitrarily redirect users from a crafted url to the login page. **CVE ID : CVE-2022-27463**	https://github.com/WWBN/AVideo/commit/77e9aa6411ff4b97571eb82e587139ec05ff894c	A-WWB-AVID-190422/365
Vendor: wztechno					
Product: wyzi					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-22	6.1	The Wyzi Theme was affected by reflected XSS vulnerabilities in the business search feature **CVE ID : CVE-2022-1164**	N/A	A-WZT-WYZI-190422/366
Vendor: Xwiki					
Product: Xwiki					
Exposure of Private Personal Information to an Unauthorized Actor	08-Apr-22	5.3	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A guest user without the right to view pages of the wiki can still list documents related to users of the wiki. The problem has been patched in XWiki versions 12.10.11, 13.4.4, and 13.9-rc-1. There is no known	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-97jg-43c9-q6pf, https://jira.xwiki.org/browse/XWIKI-18850	A-XWI-XWIK-190422/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workaround for this problem. **CVE ID : CVE-2022-24819**		
Incorrect Use of Privileged APIs	08-Apr-22	8.1	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Simple users can create global SSX/JSX without specific rights: in theory only users with Programming Rights should be allowed to create SSX or JSX that are executed everywhere on a wiki. But a bug allow anyone with edit rights to actually create those. This issue has been patched in XWiki 13.10-rc-1, 12.10.11 and 13.4.6. There's no easy workaround for this issue, administrators should upgrade their wiki. **CVE ID : CVE-2022-24821**	https://jira.xwiki.org/browse/XWIKI-19155, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-ghcq-472w-vf4h	A-XWI-XWIK-190422/368
Vendor: Yourls					
Product: Yourls					
Cross-Site Request Forgery (CSRF)	03-Apr-22	7.4	Cross-Site Request Forgery (CSRF) in GitHub repository yourls/yourls prior to 1.8.3.	https://huntr.dev/bounties/d01f0726-1a0f-4575-ae17-4b5319b11c29,	A-YOU-YOUR-190422/369

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0088	https://github.com/yourls/yourls/commit/1de256d8694b0ec7d4df2ac1d5976d4055e09d59	
Vendor: zbzcms					
Product: zbzcms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-22	6.1	zbzcms v1.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the neirong parameter at /php/ajax.php. **CVE ID : CVE-2022-27125**	N/A	A-ZBZ-ZBZC-190422/370
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Apr-22	9.8	zbzcms v1.0 was discovered to contain a SQL injection vulnerability via the art parameter at /include/make.php. **CVE ID : CVE-2022-27126**	N/A	A-ZBZ-ZBZC-190422/371
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Apr-22	6.5	zbzcms v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /php/ajax.php. **CVE ID : CVE-2022-27127**	N/A	A-ZBZ-ZBZC-190422/372
Incorrect Authorization	10-Apr-22	9.8	An incorrect access control issue at /admin/run_ajax.php in zbzcms v1.0 allows	N/A	A-ZBZ-ZBZC-190422/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to arbitrarily add administrator accounts. **CVE ID : CVE-2022-27128**		
Unrestricted Upload of File with Dangerous Type	10-Apr-22	9.8	An arbitrary file upload vulnerability at /admin/ajax.php in zbzcms v1.0 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-27129**	N/A	A-ZBZ-ZBZC-190422/374
Unrestricted Upload of File with Dangerous Type	10-Apr-22	9.8	An arbitrary file upload vulnerability at /zbzedit/php/zbz.php in zbzcms v1.0 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-27131**	N/A	A-ZBZ-ZBZC-190422/375
N/A	10-Apr-22	9.1	zbzcms v1.0 was discovered to contain an arbitrary file deletion vulnerability via /include/up.php. **CVE ID : CVE-2022-27133**	N/A	A-ZBZ-ZBZC-190422/376
Vendor: Zohocorp					
Product: manageengine_adaudit_plus					
Insufficiently Protected Credentials	05-Apr-22	8.8	Zoho ManageEngine ADAudit Plus before 7055 allows authenticated Privilege Escalation on Integrated	https://manageengine.com, https://pitstop.manageengine.com/portal/en/community/	A-ZOH-MANA-190422/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products. This occurs because a password field is present in a JSON response. **CVE ID : CVE-2022-24978**	topic/cve-2022-24978-privilege-escalation-vulnerability-manageengine-adaudit-plus	
Improper Restriction of XML External Entity Reference	05-Apr-22	9.8	Zoho ManageEngine ADAudit Plus before 7060 is vulnerable to an unauthenticated XXE attack that leads to Remote Code Execution. **CVE ID : CVE-2022-28219**	https://manageengine.com, https://www.manageengine.com/products/active-directory-audit/cve-2022-28219.html	A-ZOH-MANA-190422/378
Product: manageengine_adselfservice_plus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-22	6.1	Zoho ManageEngine ADSelfService Plus before 6121 allows XSS via the welcome name attribute to the Reset Password, Unlock Account, or User Must Change Password screen. **CVE ID : CVE-2022-24681**	https://www.manageengine.com/products/self-service-password/kb/CVE-2022-24681.html	A-ZOH-MANA-190422/379
Product: manageengine_servicedesk_plus					
Exposure of Sensitive Information to an Unauthorized Actor	05-Apr-22	5.3	Zoho ManageEngine ServiceDesk Plus before 13001 allows anyone to know the organisation's default currency name. **CVE ID : CVE-2022-25245**	https://manageengine.com, https://www.manageengine.com/products/service-desk/cve-2022-25245.html	A-ZOH-MANA-190422/380
Product: manageengine_supportcenter_plus					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-22	5.4	Zoho ManageEngine SupportCenter Plus before 11020 allows Stored XSS in the request history. **CVE ID : CVE-2022-25373**	https://manageengine.com, https://pitstop.manageengine.com/portal/en/community/topic/manageengine-supportcenter-plus-version-11-0-build-11020-released	A-ZOH-MANA-190422/381
Vendor: zoo_management_system_project					
Product: zoo_management_system					
Unrestricted Upload of File with Dangerous Type	08-Apr-22	9.8	Zoo Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via /public_html/apply_vacancy. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-27351**	N/A	A-ZOO-ZOO_-190422/382
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Apr-22	8.8	Zoo Management System v1.0 was discovered to contain a SQL injection vulnerability at /public_html/animals via the class_id parameter. **CVE ID : CVE-2022-27992**	N/A	A-ZOO-ZOO_-190422/383
Vendor: Zyxel					
Product: zyxel_ap_configurator					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-Apr-22	7.8	A local privilege escalation vulnerability caused by incorrect permission assignment in some directories of the Zyxel AP Configurator (ZAC) version 1.1.4, which could allow an attacker to execute arbitrary code as a local administrator. **CVE ID : CVE-2022-0556**	https://www.zyxel.com/support/Zyxel-security-advisory-for-local-privilege-escalation-vulnerability-of-AP-Configurator.shtml	A-ZYX-ZYXE-190422/384
Hardware					
Vendor: Asus					
Product: rt-ac86u					
Improper Input Validation	07-Apr-22	6.5	ASUS RT-AC86U has improper user request handling, which allows an unauthenticated LAN attacker to cause a denial of service by sending particular request a server-to-client reply attempt. **CVE ID : CVE-2022-25595**	N/A	H-ASU-RT-A-190422/385
Out-of-bounds Write	07-Apr-22	8.8	ASUS RT-AC56U's configuration function has a heap-based buffer overflow vulnerability due to insufficient validation for the decryption parameter length, which allows an unauthenticated LAN attacker to execute arbitrary code,	N/A	H-ASU-RT-A-190422/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform arbitrary operations and disrupt service. **CVE ID : CVE-2022-25596**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Apr-22	8.8	ASUS RT-AC86U's LPD service has insufficient filtering for special characters in the user request, which allows an unauthenticated LAN attacker to perform command injection attack, execute arbitrary commands and disrupt or terminate service. **CVE ID : CVE-2022-25597**	N/A	H-ASU-RT-A-190422/387
Product: rt-ax56u					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Apr-22	8.1	ASUS RT-AX56U's update_json function has a path traversal vulnerability due to insufficient filtering for special characters in the URL parameter. An unauthenticated LAN attacker can overwrite a system file by uploading another file with the same file name, which results in service disruption. **CVE ID : CVE-2022-23970**	N/A	H-ASU-RT-A-190422/388
Improper Limitation of a Pathname	07-Apr-22	8.1	ASUS RT-AX56U's update_PLC/PORT file has a path traversal	N/A	H-ASU-RT-A-190422/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			vulnerability due to insufficient filtering for special characters in the URL parameter. An unauthenticated LAN attacker can overwrite a system file by uploading another PLC/PORT file with the same file name, which results in service disruption. **CVE ID : CVE-2022-23971**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Apr-22	8.8	ASUS RT-AX56U's SQL handling function has an SQL injection vulnerability due to insufficient user input validation. An unauthenticated LAN attacker to inject arbitrary SQL code to read, modify and delete database. **CVE ID : CVE-2022-23972**	N/A	H-ASU-RT-A-190422/390
Out-of-bounds Write	07-Apr-22	8.8	ASUS RT-AX56U's user profile configuration function is vulnerable to stack-based buffer overflow due to insufficient validation for parameter length. An unauthenticated LAN attacker can execute arbitrary code to perform arbitrary operations or disrupt service.	N/A	H-ASU-RT-A-190422/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23973		
Vendor: Cisco					
Product: asr_5500					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Apr-22	6.7	A vulnerability in the CLI of Cisco StarOS could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient input validation of CLI commands. An attacker could exploit this vulnerability by sending crafted commands to the CLI. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the root user. To exploit this vulnerability, an attacker would need to have valid administrative credentials on an affected device. **CVE ID : CVE-2022-20665**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-staros-cmdinj-759mNT4n	H-CIS-ASR_-190422/392
Product: asr_5700					
Improper Neutralization of Special Elements used in a Command ('Comman	06-Apr-22	6.7	A vulnerability in the CLI of Cisco StarOS could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-staros-cmdinj-759mNT4n	H-CIS-ASR_-190422/393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			insufficient input validation of CLI commands. An attacker could exploit this vulnerability by sending crafted commands to the CLI. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the root user. To exploit this vulnerability, an attacker would need to have valid administrative credentials on an affected device. **CVE ID : CVE-2022-20665**		
Product: email_security_appliance					
N/A	06-Apr-22	5.3	A vulnerability in the TCP/IP stack of Cisco Email Security Appliance (ESA), Cisco Web Security Appliance (WSA), and Cisco Secure Email and Web Manager, formerly Security Management Appliance, could allow an unauthenticated, remote attacker to crash the Simple Network Management Protocol (SNMP) service, resulting in a denial of service (DoS) condition. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ESA-SNMP-JLAJksWK	H-CIS-EMAI-190422/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to an open port listener on TCP port 199. An attacker could exploit this vulnerability by connecting to TCP port 199. A successful exploit could allow the attacker to crash the SNMP service, resulting in a DoS condition. **CVE ID : CVE-2022-20675**		
Product: ip_phone_6825					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	H-CIS-IP_P-190422/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_6841					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	H-CIS-IP_P-190422/396

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_6851					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	H-CIS-IP_P-190422/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_6861					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	H-CIS-IP_P-190422/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20774		
Product: ip_phone_6871					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	H-CIS-IP_P-190422/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ip_phone_7811					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	H-CIS-IP_P-190422/400
Product: ip_phone_7821					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	H-CIS-IP_P-190422/401
Product: ip_phone_7832					
Cross-Site Request	06-Apr-22	8.1	A vulnerability in the web-based management	https://tools.cisco.com/security/center/cont	H-CIS-IP_P-190422/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**	ent/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	
Product: ip_phone_7841					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-	H-CIS-IP_P-190422/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**	phone-csrf-K56vXvVx	
Product: ip_phone_7861					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	H-CIS-IP_P-190422/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_8811					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	H-CIS-IP_P-190422/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_8832					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	H-CIS-IP_P-190422/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_8841					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	H-CIS-IP_P-190422/407

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_8845					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	H-CIS-IP_P-190422/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_8851					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	H-CIS-IP_P-190422/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_8861					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	H-CIS-IP_P-190422/410

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_8865					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	H-CIS-IP_P-190422/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: secure_email_and_web_manager					
N/A	06-Apr-22	5.3	A vulnerability in the TCP/IP stack of Cisco Email Security Appliance (ESA), Cisco Web Security Appliance (WSA), and Cisco Secure Email and Web Manager, formerly Security Management Appliance, could allow an unauthenticated, remote attacker to crash the Simple Network Management Protocol (SNMP) service, resulting in a denial of service (DoS) condition. This vulnerability is due to an open port listener on TCP port 199. An attacker could exploit this vulnerability by connecting to TCP port 199. A successful exploit could allow the attacker to crash the SNMP service, resulting in a DoS condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ESA-SNMP-JLAJksWK	H-CIS-SECU-190422/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20675		
Product: web_security_appliance					
N/A	06-Apr-22	5.3	A vulnerability in the TCP/IP stack of Cisco Email Security Appliance (ESA), Cisco Web Security Appliance (WSA), and Cisco Secure Email and Web Manager, formerly Security Management Appliance, could allow an unauthenticated, remote attacker to crash the Simple Network Management Protocol (SNMP) service, resulting in a denial of service (DoS) condition. This vulnerability is due to an open port listener on TCP port 199. An attacker could exploit this vulnerability by connecting to TCP port 199. A successful exploit could allow the attacker to crash the SNMP service, resulting in a DoS condition. **CVE ID : CVE-2022-20675**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ESA-SNMP-JLAJksWK	H-CIS-WEB_-190422/413
Improper Neutralization of Input During	06-Apr-22	5.4	A vulnerability in the web-based management interface of Cisco AsyncOS Software for	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis	H-CIS-WEB_-190422/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface. **CVE ID : CVE-2022-20781**	co-sa-wsa-stored-xss-XPsJghMY	
Improper Input Validation	06-Apr-22	5.3	A vulnerability in the Web-Based Reputation Score (WBRS) engine of Cisco AsyncOS Software for Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to bypass established	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-swa-filter-bypass-XXXTU3X	H-CIS-WEB_-190422/415

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web request policies and access blocked content on an affected device. This vulnerability is due to incorrect handling of certain character combinations inserted into a URL. An attacker could exploit this vulnerability by sending crafted URLs to be processed by an affected device. A successful exploit could allow the attacker to bypass the web proxy and access web content that has been blocked by policy. **CVE ID : CVE-2022-20784**		
Vendor: Digi					
Product: passport					
Out-of-bounds Write	06-Apr-22	7.5	Digi Passport Firmware through 1.5.1,1 is affected by a buffer overflow in the function for building the Location header string when an unauthenticated user is redirected to the authentication page. **CVE ID : CVE-2022-26952**	https://hub.digi.com/dp/path=/support/asset/digi-passport-1.5.2-firmware-release-notes/, https://hub.digi.com/support/products/infrastructure-management/digi-passport/	H-DIG-PASS-190422/416
Out-of-bounds Write	06-Apr-22	7.5	Digi Passport Firmware through 1.5.1,1 is affected by a	https://hub.digi.com/dp/path=/support/as	H-DIG-PASS-190422/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer overflow. An attacker can supply a string in the page parameter for reboot.asp endpoint, allowing him to force an overflow when the string is concatenated to the HTML body. **CVE ID : CVE-2022-26953**	set/digi-passport-1.5.2-firmware-release-notes/, https://hub.digi.com/support/products/infrastructure-management/digi-passport/	
Vendor: Dlink					
Product: dir-878					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Apr-22	8.8	D-Link DIR-878 has inadequate filtering for special characters in the webpage input field. An unauthenticated LAN attacker can perform command injection attack to execute arbitrary system commands to control the system or disrupt service. **CVE ID : CVE-2022-26670**	N/A	H-DLI-DIR--190422/418
Vendor: fantec					
Product: mwid25-ds					
Exposure of Sensitive Information to an Unauthorized Actor	06-Apr-22	7.5	FANTEC GmbH MWiD25-DS Firmware v2.000.030 allows unauthenticated attackers to access and download arbitrary files via a crafted GET request. **CVE ID : CVE-2022-26591**	N/A	H-FAN-MWID-190422/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: flexwatch					
Product: fw3170-ps-e					
Incorrect Authorization	05-Apr-22	7.5	Seyeon Tech Co., Ltd FlexWATCH FW3170-PS-E Network Video System 4.23-3000_GY allows attackers to access sensitive information. **CVE ID : CVE-2022-25584**	N/A	H-FLE-FW31-190422/420
Vendor: hitrontech					
Product: chita					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Apr-22	8.8	Hitron CHITA 7.2.2.0.3b6-CD devices contain a command injection vulnerability via the Device/DDNS ddnsUsername field. **CVE ID : CVE-2022-25017**	N/A	H-HIT-CHIT-190422/421
Vendor: mediatek					
Product: mt6580					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642.	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT65-190422/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20052		
Product: mt6735					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/423
Product: mt6737					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/424
Product: mt6739					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This	https://corp.mediatek.com/product-security-	H-MED-MT67-190422/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	bulletin/April-2022	
Product: mt6750					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/426
Product: mt6753					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642;	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**		
Product: mt6755					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/428
Product: mt6762					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/429
Product: mt6763					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory	https://corp.mediatek.com/p	H-MED-MT67-190422/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	roduct-security-bulletin/April-2022	
Product: mt6765					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/431
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**		
Out-of-bounds Write	11-Apr-22	6.5	In atf (spm), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06171715; Issue ID: ALPS06171715. **CVE ID : CVE-2022-20063**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/433
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/434
Product: mt6768					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This	https://corp.mediatek.com/product-security-	H-MED-MT67-190422/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	bulletin/April-2022	
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/436
Product: mt6769					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642;	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/438
Product: mt6771					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/439
Product: mt6779					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a	https://corp.mediatek.com/product-	H-MED-MT67-190422/440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	security-bulletin/April-2022	
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/441
Product: mt6781					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642;	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/443
Product: mt6785					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/444
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT67-190422/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	bulletin/April-2022	
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/446
Product: mt6789					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617.	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT67-190422/447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20064		
Product: mt6833					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/448
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/449
Improper Restriction of Operations within the Bounds of	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**		
Product: mt6853					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/451
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/453
Product: mt6853t					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/454
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/455

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**		
Product: mt6873					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/456
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/458
Product: mt6875					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/459
Product: mt6877					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**		
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/461
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/462
Product: mt6879					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/463
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/464
Product: mt6883					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**		
Product: mt6885					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/466
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/468
Product: mt6889					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/469
Product: mt6890					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**		
Product: mt6891					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/471
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt6893					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/473
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/474
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/475

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**		
Product: mt6895					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT68-190422/476
Product: mt6983					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT69-190422/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt6985					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT69-190422/478
Product: mt8163					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT81-190422/479
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT81-190422/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**		
Product: mt8167					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT81-190422/481
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT81-190422/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt8167s					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT81-190422/483
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT81-190422/484
Product: mt8168					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT81-190422/485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**		
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT81-190422/486
Product: mt8173					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT81-190422/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT81-190422/488
Product: mt8175					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT81-190422/489
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT81-190422/490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**		
Product: mt8183					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT81-190422/491
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT81-190422/492
Product: mt8185					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT81-190422/493
Product: mt8321					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT83-190422/494
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT83-190422/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT83-190422/496
Product: mt8362a					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT83-190422/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT83-190422/498
Product: mt8365					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT83-190422/499
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT83-190422/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**		
Product: mt8385					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT83-190422/501
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT83-190422/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	11-Apr-22	6.5	In atf (spm), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06171715; Issue ID: ALPS06171715. **CVE ID : CVE-2022-20063**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT83-190422/503
Product: mt8666					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT86-190422/504
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT86-190422/505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**		
Out-of-bounds Write	11-Apr-22	6.5	In atf (spm), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06171715; Issue ID: ALPS06171715. **CVE ID : CVE-2022-20063**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT86-190422/506
Product: mt8667					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT86-190422/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT86-190422/508
Out-of-bounds Write	11-Apr-22	6.5	In atf (spm), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06171715; Issue ID: ALPS06171715. **CVE ID : CVE-2022-20063**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT86-190422/509
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT86-190422/510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**		
Product: mt8675					
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT86-190422/511
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT86-190422/512
Product: mt8735a					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory	https://corp.mediatek.com/p	H-MED-MT87-190422/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	roduct-security-bulletin/April-2022	
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/514
Product: mt8735b					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**		
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/516
Product: mt8765					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/517
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This	https://corp.mediatek.com/product-security-	H-MED-MT87-190422/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	bulletin/April-2022	
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/519
Product: mt8766					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642;	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**		
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/521
Out-of-bounds Write	11-Apr-22	6.5	In atf (spm), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06171715; Issue ID: ALPS06171715. **CVE ID : CVE-2022-20063**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/522
Improper Restriction of Operations within the Bounds of	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**		
Product: mt8768					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/524
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418.	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20062		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/526
Product: mt8786					
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/527
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**		
Out-of-bounds Write	11-Apr-22	6.5	In atf (spm), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06171715; Issue ID: ALPS06171715. **CVE ID : CVE-2022-20063**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/529
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/530
Product: mt8788					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/531
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/532
Out-of-bounds Write	11-Apr-22	6.5	In atf (spm), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS06171715; Issue ID: ALPS06171715. **CVE ID : CVE-2022-20063**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/534
Product: mt8789					
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/535
Improper Restriction of Operations	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-190422/536

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	bulletin/April-2022	
Product: mt8791					
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/537
Product: mt8797					
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	H-MED-MT87-190422/539
Vendor: Mitsubishielectric					
Product: fx5uc					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/540

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25155		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/541
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/542

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25157		
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/543
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/544
Cleartext Storage of Sensitive	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric	https://www.mitsubishielectric.com/en/psirt/vulnerabilit	H-MIT-FX5U-190422/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	y/pdf/2021-031_en.pdf	
Product: fx5uc-32mr\/ds-ts					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/547
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/549
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/550
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**		
Product: fx5uc-32mt\/d					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/552
Use of Password Hash With	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric	https://www.mitsubishielectric.com/en/psi	H-MIT-FX5U-190422/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Computational Effort			MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	rt/vulnerability/pdf/2021-031_en.pdf	
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/554
Cleartext Storage of Sensitive	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric	https://www.mitsubishielectric.com/en/psirt/vulnerabilit	H-MIT-FX5U-190422/555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	y/pdf/2021-031_en.pdf	
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/556
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**		
Product: fx5uc-32mt\/ds-ts					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/558
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/560
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/561

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**		
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/562
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/563

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**		
Product: fx5uc-32mt\/dss					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/564
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/566
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**		
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/568
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/569

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**		
Product: fx5uc-32mt\/dss-ts					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/570
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/572
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password hash is saved in cleartext. **CVE ID : CVE-2022-25158**		
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/574
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			legitimate user's system. **CVE ID : CVE-2022-25160**		
Product: fx5uj					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/576
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			eavesdropped password hash. **CVE ID : CVE-2022-25156**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/578
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/579

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟥	**CVE ID : CVE-2022-25158**		
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/580
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/581

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25160		
Product: fx5uj-24mr\/es					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/582
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	**CVE ID : CVE-2022-25156**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/584
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/585

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/586
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: fx5uj-24mt\/es					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/588
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/590
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/591
Authentication Bypass by	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in	https://www.mitsubishielectric.com/en/psi	H-MIT-FX5U-190422/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	rt/vulnerability/pdf/2021-031_en.pdf	
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/593
Product: fx5uj-24mt\/ess					
Authentication	01-Apr-22	8.1	Use of Password Hash Instead of Password	https://www.mitsubishielect	H-MIT-FX5U-190422/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bypass by Capture-replay			for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	ric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/595
Use of Password Hash With Insufficient	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in	https://www.mitsubishielectric.com/en/psirt/vulnerabilit	H-MIT-FX5U-190422/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Computational Effort			Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	y/pdf/2021-031_en.pdf	
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/597
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/598

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**		
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/599
Product: fx5uj-40mr\/es					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/601
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**		
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/603
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**		
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/605
Product: fx5uj-40mt\/es					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/607
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**		
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/609
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the product by replay attack. **CVE ID : CVE-2022-25159**		
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/611
Product: fx5uj-40mt\/ess					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/613
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**		
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/615
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25159		
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/617
Product: fx5uj-60mr\/es					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/619
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			eavesdropped password hash. **CVE ID : CVE-2022-25157**		
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/621
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/622
Cleartext Storage of	01-Apr-22	5.9	Cleartext Storage of Sensitive Information	https://www.mitsubishielect	H-MIT-FX5U-190422/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	ric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	
Product: fx5uj-60mt\/es					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/624

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25155		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/625
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25157		
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/627
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/628
Cleartext Storage of Sensitive	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric	https://www.mitsubishielectric.com/en/psirt/vulnerabilit	H-MIT-FX5U-190422/629

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	y/pdf/2021-031_en.pdf	
Product: fx5uj-60mt\/ess					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/631
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/633
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/634
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	H-MIT-FX5U-190422/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**		
Vendor: Philips					
Product: e-alert					
Missing Authentication for Critical Function	01-Apr-22	6.5	The software does not perform any authentication for critical system functionality. **CVE ID : CVE-2022-0922**	N/A	H-PHI-E-AL-190422/636
Vendor: Rockwellautomation					
Product: compactlogix_5380					
Improper Control of Generation of Code ('Code Injection')	01-Apr-22	7.2	Rockwell Automation Studio 5000 Logix Designer (all versions) are vulnerable when an attacker who achieves administrator access on a workstation running Studio 5000 Logix Designer could inject controller code undetectable to a user.	https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-07	H-ROC-COMP-190422/637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1159		
Product: compactlogix_5480					
Improper Control of Generation of Code ('Code Injection')	01-Apr-22	7.2	Rockwell Automation Studio 5000 Logix Designer (all versions) are vulnerable when an attacker who achieves administrator access on a workstation running Studio 5000 Logix Designer could inject controller code undetectable to a user. **CVE ID : CVE-2022-1159**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-07	H-ROC-COMP-190422/638
Product: compact_guardlogix_5380					
Improper Control of Generation of Code ('Code Injection')	01-Apr-22	7.2	Rockwell Automation Studio 5000 Logix Designer (all versions) are vulnerable when an attacker who achieves administrator access on a workstation running Studio 5000 Logix Designer could inject controller code undetectable to a user. **CVE ID : CVE-2022-1159**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-07	H-ROC-COMP-190422/639
Product: controllogix_5580					
Improper Control of Generation of Code ('Code Injection')	01-Apr-22	7.2	Rockwell Automation Studio 5000 Logix Designer (all versions) are vulnerable when an attacker who achieves	https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-07	H-ROC-CONT-190422/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator access on a workstation running Studio 5000 Logix Designer could inject controller code undetectable to a user. **CVE ID : CVE-2022-1159**		
Product: guardlogix_5580					
Improper Control of Generation of Code ('Code Injection')	01-Apr-22	7.2	Rockwell Automation Studio 5000 Logix Designer (all versions) are vulnerable when an attacker who achieves administrator access on a workstation running Studio 5000 Logix Designer could inject controller code undetectable to a user. **CVE ID : CVE-2022-1159**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-07	H-ROC-GUAR-190422/641
Vendor: roku					
Product: express					
N/A	08-Apr-22	5.7	Roku devices running RokuOS v9.4.0 build 4200 or earlier that uses a Realtek WiFi chip is vulnerable to Arbitrary file modification. **CVE ID : CVE-2022-27152**	N/A	H-ROK-EXPR-190422/642
Product: express_4k\+					
N/A	08-Apr-22	5.7	Roku devices running RokuOS v9.4.0 build 4200 or earlier that uses a Realtek WiFi	N/A	H-ROK-EXPR-190422/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			chip is vulnerable to Arbitrary file modification. **CVE ID : CVE-2022-27152**		
Product: roku_tv					
N/A	08-Apr-22	5.7	Roku devices running RokuOS v9.4.0 build 4200 or earlier that uses a Realtek WiFi chip is vulnerable to Arbitrary file modification. **CVE ID : CVE-2022-27152**	N/A	H-ROK-ROKU-190422/644
Product: streambar					
N/A	08-Apr-22	5.7	Roku devices running RokuOS v9.4.0 build 4200 or earlier that uses a Realtek WiFi chip is vulnerable to Arbitrary file modification. **CVE ID : CVE-2022-27152**	N/A	H-ROK-STRE-190422/645
Product: streambar_pro					
N/A	08-Apr-22	5.7	Roku devices running RokuOS v9.4.0 build 4200 or earlier that uses a Realtek WiFi chip is vulnerable to Arbitrary file modification. **CVE ID : CVE-2022-27152**	N/A	H-ROK-STRE-190422/646
Product: streaming_stick_4k					
N/A	08-Apr-22	5.7	Roku devices running RokuOS v9.4.0 build 4200 or earlier that uses a Realtek WiFi	N/A	H-ROK-STRE-190422/647

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			chip is vulnerable to Arbitrary file modification. **CVE ID : CVE-2022-27152**		
Product: streaming_stick_4k\+					
N/A	08-Apr-22	5.7	Roku devices running RokuOS v9.4.0 build 4200 or earlier that uses a Realtek WiFi chip is vulnerable to Arbitrary file modification. **CVE ID : CVE-2022-27152**	N/A	H-ROK-STRE-190422/648
Product: ultra					
N/A	08-Apr-22	5.7	Roku devices running RokuOS v9.4.0 build 4200 or earlier that uses a Realtek WiFi chip is vulnerable to Arbitrary file modification. **CVE ID : CVE-2022-27152**	N/A	H-ROK-ULTR-190422/649
Product: wireless_speakers					
N/A	08-Apr-22	5.7	Roku devices running RokuOS v9.4.0 build 4200 or earlier that uses a Realtek WiFi chip is vulnerable to Arbitrary file modification. **CVE ID : CVE-2022-27152**	N/A	H-ROK-WIRE-190422/650
Product: wireless_subwoofer					
N/A	08-Apr-22	5.7	Roku devices running RokuOS v9.4.0 build 4200 or earlier that uses a Realtek WiFi	N/A	H-ROK-WIRE-190422/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			chip is vulnerable to Arbitrary file modification. **CVE ID : CVE-2022-27152**		
Vendor: Samsung					
Product: t5					
Uncontrolled Search Path Element	05-Apr-22	7.3	A DLL hijacking vulnerability in Samsung portable SSD T5 PC software before 1.6.9 could allow a local attacker to escalate privileges. (An attacker must already have user privileges on Windows 7, 10, or 11 to exploit this vulnerability.) **CVE ID : CVE-2022-25154**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-T5-190422/652
Vendor: Tenda					
Product: ac9					
Out-of-bounds Write	07-Apr-22	9.8	There is a stack overflow vulnerability in the SetStaticRouteCfg() function in the httpd service of Tenda AC9 15.03.2.21_cn. **CVE ID : CVE-2022-27016**	N/A	H-TEN-AC9-190422/653
Out-of-bounds Write	07-Apr-22	9.8	There is a stack overflow vulnerability in the SetSysTimeCfg() function in the httpd service of Tenda AC9 V15.03.2.21_cn. The attacker can obtain a	N/A	H-TEN-AC9-190422/654

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stable root shell through a constructed payload. **CVE ID : CVE-2022-27022**		
Vendor: ui					
Product: ua_lite					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Apr-22	10	A buffer overflow vulnerability found in the UniFi Door Access Reader Lite's (UA Lite) firmware (Version 3.8.28.24 and earlier) allows a malicious actor who has gained access to a network to control all connected UA devices. This vulnerability is fixed in Version 3.8.31.13 and later. **CVE ID : CVE-2022-22570**	https://community.ui.com/releases/Security-Advisory-Bulletin-024-024/22725557-0f72-4f5d-83b0-f16252fcd4b7	H-UI-UA_L-190422/655
Vendor: Verizon					
Product: lvskihp					
Exposure of Resource to Wrong Sphere	03-Apr-22	8.1	Verizon LVSKIHP 5G outside devices through 2022-02-15 allow anyone (knowing the device's serial number) to access a CPE admin website, e.g., at the 10.0.0.1 IP address. The password (for the verizon username) is calculated by concatenating the serial number and the model (i.e., the LVSKIHP string),	N/A	H-VER-LVSK-190422/656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running the sha256sum program, and extracting the first seven characters concatenated with the last seven characters of that SHA-256 value. **CVE ID : CVE-2022-28376**		
Vendor: wavlink					
Product: wl-wn531p3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Apr-22	9.8	A command injection vulnerability in the API of the Wavlink WL-WN531P3 router, version M31G3.V5030.201204, allows an attacker to achieve unauthorized remote code execution via a malicious POST request through /cgi-bin/adm.cgi. **CVE ID : CVE-2022-23900**	https://www.wavlink.com/en_us/product/WL-WN531P3.html	H-WAV-WL-W-190422/657
Vendor: Xerox					
Product: colorqube_8580					
Incorrect Authorization	04-Apr-22	7.5	Xerox ColorQube 8580 was discovered to contain an access control issue which allows attackers to print, view the status, and obtain sensitive information. **CVE ID : CVE-2022-26572**	N/A	H-XER-COLO-190422/658
Vendor: Zyxel					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ax7501-b0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-AX75-190422/659
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-AX75-190422/660
Product: dx5401-b0					
Improper Neutralization of Special Elements used in an OS Command ('OS	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-DX54-190422/661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-DX54-190422/662
Product: emg3525-t50b					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-EMG3-190422/663
Buffer Copy without Checking Size of Input	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A	https://www.zyxel.com/support/OS-command-injection-and-buffer-	H-ZYX-EMG3-190422/664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	overflow-vulnerabilities-of-CPE-and-ONTs.shtml	
Product: emg5523-t50b					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-EMG5-190422/665
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-EMG5-190422/666
Product: emg5723-t50k					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-EMG5-190422/667
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-EMG5-190422/668
Product: emg6726-b10a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-EMG6-190422/669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-EMG6-190422/670
Product: ep240p					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-EP24-190422/671
Buffer Copy without Checking Size of Input ('Classic	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-	H-ZYX-EP24-190422/672

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	vulnerabilities-of-CPE-and-ONTs.shtml	
Product: ex3510-b0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-EX35-190422/673
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-EX35-190422/674
Product: ex5401-b0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-EX54-190422/675
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-EX54-190422/676
Product: ex5501-b0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-EX55-190422/677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-EX55-190422/678
Product: pm7300-t0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-PM73-190422/679
Buffer Copy without Checking Size of Input ('Classic	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-	H-ZYX-PM73-190422/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	vulnerabilities-of-CPE-and-ONTs.shtml	
Product: pmg5317-t20b					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-PMG5-190422/681
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-PMG5-190422/682
Product: pmg5617-t20b2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-PMG5-190422/683
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-PMG5-190422/684
Product: pmg5617ga					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-PMG5-190422/685

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-PMG5-190422/686
Product: pmg5622ga					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-PMG5-190422/687
Buffer Copy without Checking Size of Input ('Classic	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-	H-ZYX-PMG5-190422/688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	vulnerabilities-of-CPE-and-ONTs.shtml	
Product: px7501-b0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-PX75-190422/689
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-PX75-190422/690
Product: vmg1312-t20b					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG1-190422/691
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG1-190422/692
Product: vmg3312-t20a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG3-190422/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG3-190422/694
Product: vmg3625-t50b					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG3-190422/695
Buffer Copy without Checking Size of Input ('Classic	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-	H-ZYX-VMG3-190422/696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	vulnerabilities-of-CPE-and-ONTs.shtml	
Product: vmg3927-b50a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG3-190422/697
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG3-190422/698
Product: vmg3927-b50b					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG3-190422/699
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG3-190422/700
Product: vmg3927-b60a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG3-190422/701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG3-190422/702
Product: vmg3927-t50k					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG3-190422/703
Buffer Copy without Checking Size of Input ('Classic	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-	H-ZYX-VMG3-190422/704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	vulnerabilities-of-CPE-and-ONTs.shtml	
Product: vmg4927-b50a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG4-190422/705
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG4-190422/706
Product: vmg8623-t50b					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG8-190422/707
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG8-190422/708
Product: vmg8825-b50a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG8-190422/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG8-190422/710
Product: vmg8825-b50b					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG8-190422/711
Buffer Copy without Checking Size of Input ('Classic	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-	H-ZYX-VMG8-190422/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	vulnerabilities-of-CPE-and-ONTs.shtml	
Product: vmg8825-b60a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG8-190422/713
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG8-190422/714
Product: vmg8825-b60b					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG8-190422/715
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG8-190422/716
Product: vmg8825-t50k					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG8-190422/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-VMG8-190422/718
Product: xmg3927-b50a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-XMG3-190422/719
Buffer Copy without Checking Size of Input ('Classic	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-	H-ZYX-XMG3-190422/720

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	vulnerabilities-of-CPE-and-ONTs.shtml	
Product: xmg8825-b50a					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-XMG8-190422/721
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	H-ZYX-XMG8-190422/722
Operating System					
Vendor: Asus					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: rt-ac86u_firmware					
Improper Input Validation	07-Apr-22	6.5	ASUS RT-AC86U has improper user request handling, which allows an unauthenticated LAN attacker to cause a denial of service by sending particular request a server-to-client reply attempt. **CVE ID : CVE-2022-25595**	N/A	O-ASU-RT-A-190422/723
Out-of-bounds Write	07-Apr-22	8.8	ASUS RT-AC56U's configuration function has a heap-based buffer overflow vulnerability due to insufficient validation for the decryption parameter length, which allows an unauthenticated LAN attacker to execute arbitrary code, perform arbitrary operations and disrupt service. **CVE ID : CVE-2022-25596**	N/A	O-ASU-RT-A-190422/724
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Apr-22	8.8	ASUS RT-AC86U's LPD service has insufficient filtering for special characters in the user request, which allows an unauthenticated LAN attacker to perform command injection attack, execute arbitrary commands	N/A	O-ASU-RT-A-190422/725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and disrupt or terminate service. **CVE ID : CVE-2022-25597**		
Product: rt-ax56u_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Apr-22	8.1	ASUS RT-AX56U's update_json function has a path traversal vulnerability due to insufficient filtering for special characters in the URL parameter. An unauthenticated LAN attacker can overwrite a system file by uploading another file with the same file name, which results in service disruption. **CVE ID : CVE-2022-23970**	N/A	O-ASU-RT-A-190422/726
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Apr-22	8.1	ASUS RT-AX56U's update_PLC/PORT file has a path traversal vulnerability due to insufficient filtering for special characters in the URL parameter. An unauthenticated LAN attacker can overwrite a system file by uploading another PLC/PORT file with the same file name, which results in service disruption. **CVE ID : CVE-2022-23971**	N/A	O-ASU-RT-A-190422/727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Apr-22	8.8	ASUS RT-AX56U's SQL handling function has an SQL injection vulnerability due to insufficient user input validation. An unauthenticated LAN attacker to inject arbitrary SQL code to read, modify and delete database. **CVE ID : CVE-2022-23972**	N/A	O-ASU-RT-A-190422/728
Out-of-bounds Write	07-Apr-22	8.8	ASUS RT-AX56U's user profile configuration function is vulnerable to stack-based buffer overflow due to insufficient validation for parameter length. An unauthenticated LAN attacker can execute arbitrary code to perform arbitrary operations or disrupt service. **CVE ID : CVE-2022-23973**	N/A	O-ASU-RT-A-190422/729
Vendor: Cisco					
Product: asyncos					
N/A	06-Apr-22	5.3	A vulnerability in the TCP/IP stack of Cisco Email Security Appliance (ESA), Cisco Web Security Appliance (WSA), and Cisco Secure Email and Web Manager, formerly Security Management Appliance, could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ESA-SNMP-JLAJksWK	O-CIS-ASYN-190422/730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, remote attacker to crash the Simple Network Management Protocol (SNMP) service, resulting in a denial of service (DoS) condition. This vulnerability is due to an open port listener on TCP port 199. An attacker could exploit this vulnerability by connecting to TCP port 199. A successful exploit could allow the attacker to crash the SNMP service, resulting in a DoS condition. **CVE ID : CVE-2022-20675**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-22	5.4	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. The vulnerability exists because the web-based management interface does not	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-stored-xss-XPsJghMY	O-CIS-ASYN-190422/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			properly validate user-supplied input. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface. **CVE ID : CVE-2022-20781**		
Product: ip_phone_6825_firmware					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	O-CIS-IP_P-190422/732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_6841_firmware					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	O-CIS-IP_P-190422/733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_6851_firmware					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	O-CIS-IP_P-190422/734

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_6861_firmware					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	O-CIS-IP_P-190422/735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_6871_firmware					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	O-CIS-IP_P-190422/736

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20774		
Product: ip_phone_7811_firmware					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	O-CIS-IP_P-190422/737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ip_phone_7821_firmware					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	O-CIS-IP_P-190422/738
Product: ip_phone_7832_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	O-CIS-IP_P-190422/739
Product: ip_phone_7841_firmware					
Cross-Site Request	06-Apr-22	8.1	A vulnerability in the web-based management	https://tools.cisco.com/security/center/cont	O-CIS-IP_P-190422/740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**	ent/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	
Product: ip_phone_7861_firmware					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-	O-CIS-IP_P-190422/741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**	phone-csrf-K56vXvVx	
Product: ip_phone_8811_firmware					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	O-CIS-IP_P-190422/742

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_8832_firmware					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	O-CIS-IP_P-190422/743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_8841_firmware					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	O-CIS-IP_P-190422/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_8845_firmware					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	O-CIS-IP_P-190422/745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_8851_firmware					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	O-CIS-IP_P-190422/746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_8861_firmware					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	O-CIS-IP_P-190422/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: ip_phone_8865_firmware					
Cross-Site Request Forgery (CSRF)	06-Apr-22	8.1	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx	O-CIS-IP_P-190422/748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20774**		
Product: staros					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Apr-22	6.7	A vulnerability in the CLI of Cisco StarOS could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient input validation of CLI commands. An attacker could exploit this vulnerability by sending crafted commands to the CLI. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the root user. To exploit this vulnerability, an attacker would need to have valid administrative credentials on an affected device. **CVE ID : CVE-2022-20665**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-staros-cmdinj-759mNT4n	O-CIS-STAR-190422/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Dell					
Product: emc_powerscale_onefs					
N/A	08-Apr-22	4.4	Dell EMC Powerscale OneFS 8.2.x - 9.2.x omit security-relevant information in /etc/master.passwd. A high-privileged user can exploit this vulnerability to not record information identifying the source of account information changes. **CVE ID : CVE-2022-22563**	https://www.dell.com/support/kbdoc/000196657, https://www.dell.com/support/kbdoc/en-an/000197991/dell-emc-powerscale-onefs-security-update-for-multiple-component-vulnerabilities	O-DEL-EMC_-190422/750
Improper Preservation of Permissions	08-Apr-22	8.8	Dell PowerScale OneFS, versions 8.2.x, 9.0.0.x, 9.1.0.x, 9.2.0.x, 9.2.1.x, and 9.3.0.x, contain an improper preservation of privileges. A remote filesystem user with a local account could potentially exploit this vulnerability, leading to an escalation of file privileges and information disclosure. **CVE ID : CVE-2022-24428**	https://www.dell.com/support/kbdoc/en-us/000197991/dell-emc-powerscale-onefs-security-update-for-multiple-component-vulnerabilities	O-DEL-EMC_-190422/751
Use of Insufficiently Random Values	08-Apr-22	9.1	Dell PowerScale OneFS, 8.2.2-9.3.x, contains a predictable file name from observable state vulnerability. An unprivileged network	https://www.dell.com/support/kbdoc/en-us/000197991/dell-emc-powerscale-onefs-security-	O-DEL-EMC_-190422/752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could potentially exploit this vulnerability, leading to data loss. **CVE ID : CVE-2022-26851**	update-for-multiple-component-vulnerabilities	
Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)	08-Apr-22	9.8	Dell PowerScale OneFS, versions 8.2.x-9.3.x, contain a predictable seed in pseudo-random number generator. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to an account compromise. **CVE ID : CVE-2022-26852**	https://www.dell.com/support/kbdoc/en-us/000197991/dell-emc-powerscale-onefs-security-update-for-multiple-component-vulnerabilities	O-DEL-EMC_-190422/753
Use of a Broken or Risky Cryptographic Algorithm	08-Apr-22	9.8	Dell PowerScale OneFS, versions 8.2.x-9.2.x, contain risky cryptographic algorithms. A remote unprivileged malicious attacker could potentially exploit this vulnerability, leading to full system access **CVE ID : CVE-2022-26854**	https://www.dell.com/support/kbdoc/en-us/000197991/dell-emc-powerscale-onefs-security-update-for-multiple-component-vulnerabilities	O-DEL-EMC_-190422/754
Incorrect Default Permissions	08-Apr-22	5.5	Dell PowerScale OneFS, versions 8.2.x-9.3.0.x, contains an incorrect default permissions vulnerability. A local malicious user could potentially exploit	https://www.dell.com/support/kbdoc/en-us/000197991/dell-emc-powerscale-onefs-security-update-for-	O-DEL-EMC_-190422/755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability, leading to a denial of service. **CVE ID : CVE-2022-26855**	multiple-component-vulnerabilities	
Vendor: Digi					
Product: passport_firmware					
Out-of-bounds Write	06-Apr-22	7.5	Digi Passport Firmware through 1.5.1,1 is affected by a buffer overflow in the function for building the Location header string when an unauthenticated user is redirected to the authentication page. **CVE ID : CVE-2022-26952**	https://hub.digi.com/dp/path=/support/asset/digi-passport-1.5.2-firmware-release-notes/, https://hub.digi.com/support/products/infrastructure-management/digi-passport/	O-DIG-PASS-190422/756
Out-of-bounds Write	06-Apr-22	7.5	Digi Passport Firmware through 1.5.1,1 is affected by a buffer overflow. An attacker can supply a string in the page parameter for reboot.asp endpoint, allowing him to force an overflow when the string is concatenated to the HTML body. **CVE ID : CVE-2022-26953**	https://hub.digi.com/dp/path=/support/asset/digi-passport-1.5.2-firmware-release-notes/, https://hub.digi.com/support/products/infrastructure-management/digi-passport/	O-DIG-PASS-190422/757
Vendor: Dlink					
Product: dir-878_firmware					
Improper Neutralization of Special Elements	07-Apr-22	8.8	D-Link DIR-878 has inadequate filtering for special characters in the webpage input field. An	N/A	O-DLI-DIR--190422/758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			unauthenticated LAN attacker can perform command injection attack to execute arbitrary system commands to control the system or disrupt service. **CVE ID : CVE-2022-26670**		
Vendor: fantec					
Product: mwid25-ds_firmware					
Exposure of Sensitive Information to an Unauthorized Actor	06-Apr-22	7.5	FANTEC GmbH MWiD25-DS Firmware v2.000.030 allows unauthenticated attackers to access and download arbitrary files via a crafted GET request. **CVE ID : CVE-2022-26591**	N/A	O-FAN-MWID-190422/759
Vendor: Fedoraproject					
Product: fedora					
Incorrect Default Permissions	04-Apr-22	7.5	A flaw was found in crun where containers were incorrectly started with non-empty default permissions. A vulnerability was found in Moby (Docker Engine) where containers were started incorrectly with non-empty inheritable Linux process capabilities. This flaw allows an attacker	https://github.com/containers/crun/commit/1aeeed2e4fdeffb4875c0d0b439915894594c8c6	O-FED-FEDO-190422/760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs. **CVE ID : CVE-2022-27650**		
Incorrect Default Permissions	04-Apr-22	6.8	A flaw was found in buildah where containers were incorrectly started with non-empty default permissions. A bug was found in Moby (Docker Engine) where containers were incorrectly started with non-empty inheritable Linux process capabilities, enabling an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs. This has the potential to impact confidentiality and integrity. **CVE ID : CVE-2022-27651**	https://github.com/containers/buildah/commit/e7e55c988c05dd74005184ceb64f097a0cfe645b	O-FED-FEDO-190422/761
Use After Free	08-Apr-22	7	jbd2_journal_wait_updates in fs/jbd2/transaction.c in the Linux kernel before 5.17.1 has a use-after-free caused	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.17.1, https://github.	O-FED-FEDO-190422/762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by a transaction_t race condition. **CVE ID : CVE-2022-28796**	com/torvalds/linux/commit/cc16eecae687912238ee6efbff71ad31e2bc414e	
Vendor: flexwatch					
Product: fw3170-ps-e_firmware					
Incorrect Authorization	05-Apr-22	7.5	Seyeon Tech Co., Ltd FlexWATCH FW3170-PS-E Network Video System 4.23-3000_GY allows attackers to access sensitive information. **CVE ID : CVE-2022-25584**	N/A	O-FLE-FW31-190422/763
Vendor: Google					
Product: android					
Improper Input Validation	05-Apr-22	6.5	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 98.0.4758.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2022-0455**	https://crbug.com/1270593, https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html	O-GOO-ANDR-190422/764
N/A	05-Apr-22	6.5	Inappropriate implementation in Full screen mode in Google Chrome on Android prior to 99.0.4844.51 allowed a remote attacker to hide the contents of the Omnibox (URL	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1270052	O-GOO-ANDR-190422/765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bar) via a crafted HTML page. **CVE ID : CVE-2022-0802**		
N/A	05-Apr-22	6.5	Inappropriate implementation in Full screen mode in Google Chrome on Android prior to 99.0.4844.51 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2022-0804**	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html, https://crbug.com/1264561	O-GOO-ANDR-190422/766
Use After Free	11-Apr-22	6.5	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642. **CVE ID : CVE-2022-20052**	https://corp.mediatek.com/product-security-bulletin/April-2022	O-GOO-ANDR-190422/767
Use After Free	11-Apr-22	6.7	In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/April-2022	O-GOO-ANDR-190422/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418. **CVE ID : CVE-2022-20062**		
Out-of-bounds Write	11-Apr-22	6.5	In atf (spm), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06171715; Issue ID: ALPS06171715. **CVE ID : CVE-2022-20063**	https://corp.mediatek.com/product-security-bulletin/April-2022	O-GOO-ANDR-190422/769
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Apr-22	6.7	In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617. **CVE ID : CVE-2022-20064**	https://corp.mediatek.com/product-security-bulletin/April-2022	O-GOO-ANDR-190422/770
Product: chrome_os					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	05-Apr-22	8.8	Use after free in File Manager in Google Chrome on Chrome OS prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-0603**	https://crbug.com/1290008, https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html	O-GOO-CHRO-190422/771
Vendor: hitrontech					
Product: chita_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Apr-22	8.8	Hitron CHITA 7.2.2.0.3b6-CD devices contain a command injection vulnerability via the Device/DDNS ddnsUsername field. **CVE ID : CVE-2022-25017**	N/A	O-HIT-CHIT-190422/772
Vendor: Linux					
Product: linux_kernel					
Double Free	03-Apr-22	7.8	usb_8dev_start_xmit in drivers/net/can/usb/usb_8dev.c in the Linux kernel through 5.17.1 has a double free. **CVE ID : CVE-2022-28388**	https://github.com/torvalds/linux/commit/3d3925ff6433f98992685a9679613a2cc97f3ce2	O-LIN-LINU-190422/773
Double Free	03-Apr-22	7.8	mcba_usb_start_xmit in drivers/net/can/usb/mcba_usb.c in the Linux kernel through	https://github.com/torvalds/linux/commit/04c9b00ba83594a29813d6b1	O-LIN-LINU-190422/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5.17.1 has a double free. **CVE ID : CVE-2022-28389**	fb8fdc93a3915174	
Double Free	03-Apr-22	7.8	ems_usb_start_xmit in drivers/net/can/usb/ems_usb.c in the Linux kernel through 5.17.1 has a double free. **CVE ID : CVE-2022-28390**	https://github.com/torvalds/linux/commit/c70222752228a62135cee3409dccefd494a24646	O-LIN-LINU-190422/775
Use After Free	08-Apr-22	7	jbd2_journal_wait_updates in fs/jbd2/transaction.c in the Linux kernel before 5.17.1 has a use-after-free caused by a transaction_t race condition. **CVE ID : CVE-2022-28796**	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.17.1, https://github.com/torvalds/linux/commit/cc16eecae687912238ee6efbff71ad31e2bc414e	O-LIN-LINU-190422/776
Use After Free	11-Apr-22	7.8	The SUNRPC subsystem in the Linux kernel through 5.17.2 can call xs_xprt_free before ensuring that sockets are in the intended state. **CVE ID : CVE-2022-28893**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=1a3b1bba7c7a5eb8a11513cf88427cb9d77bc60a, http://www.openwall.com/lists/oss-security/2022/04/11/4, http://www.openwall.com/lists/oss-	O-LIN-LINU-190422/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				security/2022/04/11/3	
Vendor: Microsoft					
Product: windows					
Unquoted Search Path or Element	05-Apr-22	7.8	There is an unquoted service path in Sherpa Connector Service (SherpaConnectorService.exe) 2020.2.20328.2050. This might allow a local user to escalate privileges by creating a "C:\Program Files\Sherpa Software\Sherpa.exe" file. **CVE ID : CVE-2022-23909**	N/A	O-MIC-WIND-190422/778
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Apr-22	9.8	In Apache Hadoop, The unTar function uses unTarUsingJava function on Windows and the built-in tar utility on Unix and other OSes. As a result, a TAR entry may create a symlink under the expected extraction directory which points to an external directory. A subsequent TAR entry may extract an arbitrary file into the external directory using the symlink name. This however would be caught by the same targetDirPath check on Unix because of	https://lists.apache.org/thread/hslo7wzw2449gv1jyjk8g6ttd7935fyz	O-MIC-WIND-190422/779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the getCanonicalPath call. However on Windows, getCanonicalPath doesn't resolve symbolic links, which bypasses the check. unpackEntries during TAR extraction follows symbolic links which allows writing outside expected base directory on Windows. This was addressed in Apache Hadoop 3.2.3 **CVE ID : CVE-2022-26612**		
Unrestricted Upload of File with Dangerous Type	11-Apr-22	9.8	In Studio-42 elFinder 2.1.60, there is a vulnerability that causes remote code execution through file name bypass for file upload. **CVE ID : CVE-2022-27115**	https://github.com/Studio-42/elFinder/issues/3458	O-MIC-WIND-190422/780
Vendor: Mitsubishielectric					
Product: fx5uc-32mr\/ds-ts_firmware					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/782
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**		
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/784
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25159		
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/786
Product: fx5uc-32mt\/ds-ts_firmware					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/788
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			eavesdropped password hash. **CVE ID : CVE-2022-25157**		
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/790
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/791
Cleartext Storage of	01-Apr-22	5.9	Cleartext Storage of Sensitive Information	https://www.mitsubishielect	O-MIT-FX5U-190422/792

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	ric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	
Product: fx5uc-32mt\/dss-ts_firmware					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25155		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/794
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25157		
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/796
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/797
Cleartext Storage of Sensitive	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric	https://www.mitsubishielectric.com/en/psirt/vulnerabilit	O-MIT-FX5U-190422/798

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	y/pdf/2021-031_en.pdf	
Product: fx5uc-32mt\/dss_firmware					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/800
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/802
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/803
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**		
Product: fx5uc-32mt\/d_firmware					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/805
Use of Password Hash With	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric	https://www.mitsubishielectric.com/en/psi	O-MIT-FX5U-190422/806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Computational Effort			MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	rt/vulnerability/pdf/2021-031_en.pdf	
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/807
Cleartext Storage of Sensitive	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric	https://www.mitsubishielectric.com/en/psirt/vulnerabilit	O-MIT-FX5U-190422/808

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	y/pdf/2021-031_en.pdf	
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/809
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**		
Product: fx5uc_firmware					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/811
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/813
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**		
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/815
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/816

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**		
Product: fx5uj-24mr\/es_firmware					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/817
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/819
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**		
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/821
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**		
Product: fx5uj-24mt\/ess_firmware					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/823
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/825
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password hash is saved in cleartext. **CVE ID : CVE-2022-25158**		
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/827
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			legitimate user's system. **CVE ID : CVE-2022-25160**		
Product: fx5uj-24mt\/es_firmware					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/829
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			eavesdropped password hash. **CVE ID : CVE-2022-25156**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/831
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25158		
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/833
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25160		
Product: fx5uj-40mr\/es_firmware					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/835
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25156		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/837
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/838

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/839
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: fx5uj-40mt\/ess_firmware					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/841
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/842

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/843
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/844
Authentication Bypass by	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in	https://www.mitsubishielectric.com/en/psi	O-MIT-FX5U-190422/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	rt/vulnerability/pdf/2021-031_en.pdf	
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/846
Product: fx5uj-40mt\/es_firmware					
Authentication	01-Apr-22	8.1	Use of Password Hash Instead of Password	https://www.mitsubishielect	O-MIT-FX5U-190422/847

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bypass by Capture-replay			for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**	ric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/848
Use of Password Hash With Insufficient	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in	https://www.mitsubishielectric.com/en/psirt/vulnerabilit	O-MIT-FX5U-190422/849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Computational Effort			Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**	y/pdf/2021-031_en.pdf	
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/850
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**		
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/852
Product: fx5uj-60mr\/es_firmware					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/854
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/855

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**		
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/856
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**		
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/858
Product: fx5uj-60mt\/ess_firmware					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/860
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**		
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/862
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the product by replay attack. **CVE ID : CVE-2022-25159**		
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/864
Product: fx5uj-60mt\/es_firmware					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to login to the product by replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/866
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tamper with the information in the product by using an eavesdropped password hash. **CVE ID : CVE-2022-25157**		
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/868
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25159		
Cleartext Storage of Sensitive Information	01-Apr-22	5.9	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/870
Product: fx5uj_firmware					
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			replaying an eavesdropped password hash. **CVE ID : CVE-2022-25155**		
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	8.1	Use of Weak Hash vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash. **CVE ID : CVE-2022-25156**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/872
Use of Password Hash With Insufficient Computational Effort	01-Apr-22	9.1	Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			eavesdropped password hash. **CVE ID : CVE-2022-25157**		
Cleartext Storage of Sensitive Information	01-Apr-22	9.1	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote attacker to disclose or tamper with a file in which password hash is saved in cleartext. **CVE ID : CVE-2022-25158**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/874
Authentication Bypass by Capture-replay	01-Apr-22	8.1	Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack. **CVE ID : CVE-2022-25159**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	O-MIT-FX5U-190422/875
Cleartext Storage of	01-Apr-22	5.9	Cleartext Storage of Sensitive Information	https://www.mitsubishielect	O-MIT-FX5U-190422/876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			vulnerability in Mitsubishi Electric MELSEC iQ-F series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series FX5UJ CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system. **CVE ID : CVE-2022-25160**	ric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf	
Vendor: Philips					
Product: e-alert_firmware					
Missing Authentication for Critical Function	01-Apr-22	6.5	The software does not perform any authentication for critical system functionality. **CVE ID : CVE-2022-0922**	N/A	O-PHI-E-AL-190422/877
Vendor: Redhat					
Product: enterprise_linux					
Incorrect Default Permissions	04-Apr-22	7.5	A flaw was found in Podman, where containers were started incorrectly with non-empty default permissions. A vulnerability was found in Moby	https://github.com/containers/podman/commit/aafa80918a245edcbdaceb1191d749570f1872d0	O-RED-ENTE-190422/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Docker Engine), where containers were started incorrectly with non-empty inheritable Linux process capabilities. This flaw allows an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs. **CVE ID : CVE-2022-27649**		
Incorrect Default Permissions	04-Apr-22	7.5	A flaw was found in crun where containers were incorrectly started with non-empty default permissions. A vulnerability was found in Moby (Docker Engine) where containers were started incorrectly with non-empty inheritable Linux process capabilities. This flaw allows an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs. **CVE ID : CVE-2022-27650**	https://github.com/containers/crun/commit/1aeeed2e4fdeffb4875c0d0b439915894594c8c6	O-RED-ENTE-190422/879

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	04-Apr-22	6.8	A flaw was found in buildah where containers were incorrectly started with non-empty default permissions. A bug was found in Moby (Docker Engine) where containers were incorrectly started with non-empty inheritable Linux process capabilities, enabling an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs. This has the potential to impact confidentiality and integrity. **CVE ID : CVE-2022-27651**	https://github.com/containers/buildah/commit/e7e55c988c05dd74005184ceb64f097a0cfe645b	O-RED-ENTE-190422/880
Use After Free	08-Apr-22	7	jbd2_journal_wait_updates in fs/jbd2/transaction.c in the Linux kernel before 5.17.1 has a use-after-free caused by a transaction_t race condition. **CVE ID : CVE-2022-28796**	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.17.1, https://github.com/torvalds/linux/commit/cc16eecae687912238ee6efbff71ad31e2bc414e	O-RED-ENTE-190422/881
Vendor: Rockwellautomation					
Product: compactlogix_5380_firmware					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	01-Apr-22	7.2	Rockwell Automation Studio 5000 Logix Designer (all versions) are vulnerable when an attacker who achieves administrator access on a workstation running Studio 5000 Logix Designer could inject controller code undetectable to a user. **CVE ID : CVE-2022-1159**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-07	O-ROC-COMP-190422/882
Product: compactlogix_5480_firmware					
Improper Control of Generation of Code ('Code Injection')	01-Apr-22	7.2	Rockwell Automation Studio 5000 Logix Designer (all versions) are vulnerable when an attacker who achieves administrator access on a workstation running Studio 5000 Logix Designer could inject controller code undetectable to a user. **CVE ID : CVE-2022-1159**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-07	O-ROC-COMP-190422/883
Product: compact_guardlogix_5380_firmware					
Improper Control of Generation of Code ('Code Injection')	01-Apr-22	7.2	Rockwell Automation Studio 5000 Logix Designer (all versions) are vulnerable when an attacker who achieves administrator access on a workstation running Studio 5000 Logix Designer could	https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-07	O-ROC-COMP-190422/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject controller code undetectable to a user. **CVE ID : CVE-2022-1159**		
Product: controllogix_5580_firmware					
Improper Control of Generation of Code ('Code Injection')	01-Apr-22	7.2	Rockwell Automation Studio 5000 Logix Designer (all versions) are vulnerable when an attacker who achieves administrator access on a workstation running Studio 5000 Logix Designer could inject controller code undetectable to a user. **CVE ID : CVE-2022-1159**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-07	O-ROC-CONT-190422/885
Product: guardlogix_5580_firmware					
Improper Control of Generation of Code ('Code Injection')	01-Apr-22	7.2	Rockwell Automation Studio 5000 Logix Designer (all versions) are vulnerable when an attacker who achieves administrator access on a workstation running Studio 5000 Logix Designer could inject controller code undetectable to a user. **CVE ID : CVE-2022-1159**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-07	O-ROC-GUAR-190422/886
Product: safety_instrumented_systems_workstation					
Improper Restriction of XML	01-Apr-22	5.5	When opening a malicious solution file provided by an	https://www.cisa.gov/uscert/	O-ROC-SAFE-190422/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
External Entity Reference			attacker, the application suffers from an XML external entity vulnerability due to an unsafe call within a dynamic link library file. An attacker could exploit this to pass data from local files to a remote web server, leading to a loss of confidentiality. **CVE ID : CVE-2022-1018**	ics/advisories/icsa-22-088-01	
Vendor: roku					
Product: roku_os					
N/A	08-Apr-22	5.7	Roku devices running RokuOS v9.4.0 build 4200 or earlier that uses a Realtek WiFi chip is vulnerable to Arbitrary file modification. **CVE ID : CVE-2022-27152**	N/A	O-ROK-ROKU-190422/888
Vendor: Samsung					
Product: t5_firmware					
Uncontrolled Search Path Element	05-Apr-22	7.3	A DLL hijacking vulnerability in Samsung portable SSD T5 PC software before 1.6.9 could allow a local attacker to escalate privileges. (An attacker must already have user privileges on Windows 7, 10, or 11 to exploit this vulnerability.)	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-T5_F-190422/889

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25154		
Vendor: Tenda					
Product: ac9_firmware					
Out-of-bounds Write	07-Apr-22	9.8	There is a stack overflow vulnerability in the SetStaticRouteCfg() function in the httpd service of Tenda AC9 15.03.2.21_cn. **CVE ID : CVE-2022-27016**	N/A	O-TEN-AC9_-190422/890
Out-of-bounds Write	07-Apr-22	9.8	There is a stack overflow vulnerability in the SetSysTimeCfg() function in the httpd service of Tenda AC9 V15.03.2.21_cn. The attacker can obtain a stable root shell through a constructed payload. **CVE ID : CVE-2022-27022**	N/A	O-TEN-AC9_-190422/891
Vendor: ui					
Product: ua_lite_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Apr-22	10	A buffer overflow vulnerability found in the UniFi Door Access Reader Lite's (UA Lite) firmware (Version 3.8.28.24 and earlier) allows a malicious actor who has gained access to a network to control all connected UA devices. This vulnerability is	https://community.ui.com/releases/Security-Advisory-Bulletin-024-024/22725557-0f72-4f5d-83b0-f16252fcd4b7	O-UI-UA_L-190422/892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in Version 3.8.31.13 and later. **CVE ID : CVE-2022-22570**		
Vendor: Verizon					
Product: lvskihp_firmware					
Exposure of Resource to Wrong Sphere	03-Apr-22	8.1	Verizon LVSKIHP 5G outside devices through 2022-02-15 allow anyone (knowing the device's serial number) to access a CPE admin website, e.g., at the 10.0.0.1 IP address. The password (for the verizon username) is calculated by concatenating the serial number and the model (i.e., the LVSKIHP string), running the sha256sum program, and extracting the first seven characters concatenated with the last seven characters of that SHA-256 value. **CVE ID : CVE-2022-28376**	N/A	O-VER-LVSK-190422/893
Vendor: wavlink					
Product: wl-wn531p3_firmware					
Improper Neutralization of Special Elements used in a Command	07-Apr-22	9.8	A command injection vulnerability in the API of the Wavlink WL-WN531P3 router, version M31G3.V5030.201204, allows an attacker	https://www.wavlink.com/en_us/product/WL-WN531P3.html	O-WAV-WL-W-190422/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			to achieve unauthorized remote code execution via a malicious POST request through /cgi-bin/adm.cgi. **CVE ID : CVE-2022-23900**		
Vendor: XEN					
Product: xen					
Missing Release of Resource after Effective Lifetime	05-Apr-22	5.6	Racy interactions between dirty vram tracking and paging log dirty hypercalls Activation of log dirty mode done by XEN_DMOP_track_dirty_vram (was named HVMOP_track_dirty_vram before Xen 4.9) is racy with ongoing log dirty hypercalls. A suitably timed call to XEN_DMOP_track_dirty_vram can enable log dirty while another CPU is still in the process of tearing down the structures related to a previously enabled log dirty mode (XEN_DOMCTL_SHADOW_OP_OFF). This is due to lack of mutually exclusive locking between both operations and can lead to entries being added in already freed slots, resulting in a memory leak.	http://xenbits.xen.org/xsa/advisory-397.html, http://www.openwall.com/lists/oss-security/2022/04/05/1	O-XEN-XEN-190422/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26356		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	05-Apr-22	7	race in VT-d domain ID cleanup Xen domain IDs are up to 15 bits wide. VT-d hardware may allow for only less than 15 bits to hold a domain ID associating a physical device with a particular domain. Therefore internally Xen domain IDs are mapped to the smaller value range. The cleaning up of the housekeeping structures has a race, allowing for VT-d domain IDs to be leaked and flushes to be bypassed. **CVE ID : CVE-2022-26357**	https://xenbits.xenproject.org/xsa/advisory-399.txt, http://xenbits.xen.org/xsa/advisory-399.html, http://www.openwall.com/lists/oss-security/2022/04/05/2	O-XEN-XEN-190422/896
N/A	05-Apr-22	7.8	IOMMU: RMRR (VT-d) and unity map (AMD-Vi) handling issues T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Certain PCI devices in a system might be assigned Reserved Memory Regions (specified via Reserved Memory Region Reporting, "RMRR") for Intel VT-	https://xenbits.xenproject.org/xsa/advisory-400.txt, http://xenbits.xen.org/xsa/advisory-400.html, http://www.openwall.com/lists/oss-security/2022/04/05/3	O-XEN-XEN-190422/897

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			d or Unity Mapping ranges for AMD-Vi. These are typically used for platform tasks such as legacy USB emulation. Since the precise purpose of these regions is unknown, once a device associated with such a region is active, the mappings of these regions need to remain continuouly accessible by the device. This requirement has been violated. Subsequent DMA or interrupts from the device may have unpredictable behaviour, ranging from IOMMU faults to memory corruption. **CVE ID : CVE-2022-26358**		
N/A	05-Apr-22	7.8	IOMMU: RMRR (VT-d) and unity map (AMD-Vi) handling issues T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Certain PCI devices in a system might be assigned Reserved Memory Regions (specified via Reserved Memory Region Reporting,	https://xenbits.xenproject.org/xsa/advisory-400.txt, http://xenbits.xen.org/xsa/advisory-400.html, http://www.openwall.com/lists/oss-security/2022/04/05/3	O-XEN-XEN-190422/898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"RMRR") for Intel VT-d or Unity Mapping ranges for AMD-Vi. These are typically used for platform tasks such as legacy USB emulation. Since the precise purpose of these regions is unknown, once a device associated with such a region is active, the mappings of these regions need to remain continuouly accessible by the device. This requirement has been violated. Subsequent DMA or interrupts from the device may have unpredictable behaviour, ranging from IOMMU faults to memory corruption. **CVE ID : CVE-2022-26359**		
N/A	05-Apr-22	7.8	IOMMU: RMRR (VT-d) and unity map (AMD-Vi) handling issues T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Certain PCI devices in a system might be assigned Reserved Memory Regions (specified via Reserved Memory	https://xenbits.xenproject.org/xsa/advisory-400.txt, http://xenbits.xen.org/xsa/advisory-400.html, http://www.openwall.com/lists/oss-security/2022/04/05/3	O-XEN-XEN-190422/899

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Region Reporting, "RMRR") for Intel VT-d or Unity Mapping ranges for AMD-Vi. These are typically used for platform tasks such as legacy USB emulation. Since the precise purpose of these regions is unknown, once a device associated with such a region is active, the mappings of these regions need to remain continuouly accessible by the device. This requirement has been violated. Subsequent DMA or interrupts from the device may have unpredictable behaviour, ranging from IOMMU faults to memory corruption. **CVE ID : CVE-2022-26360**		
N/A	05-Apr-22	7.8	IOMMU: RMRR (VT-d) and unity map (AMD-Vi) handling issues T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Certain PCI devices in a system might be assigned Reserved Memory Regions (specified via	https://xenbits.xenproject.org/xsa/advisory-400.txt, http://xenbits.xen.org/xsa/advisory-400.html, http://www.openwall.com/lists/oss-security/2022/04/05/3	O-XEN-XEN-190422/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Reserved Memory Region Reporting, "RMRR") for Intel VT-d or Unity Mapping ranges for AMD-Vi. These are typically used for platform tasks such as legacy USB emulation. Since the precise purpose of these regions is unknown, once a device associated with such a region is active, the mappings of these regions need to remain continuouly accessible by the device. This requirement has been violated. Subsequent DMA or interrupts from the device may have unpredictable behaviour, ranging from IOMMU faults to memory corruption. **CVE ID : CVE-2022-26361**		
Vendor: Xerox					
Product: colorqube_8580_firmware					
Incorrect Authorization	04-Apr-22	7.5	Xerox ColorQube 8580 was discovered to contain an access control issue which allows attackers to print, view the status, and obtain sensitive information. **CVE ID : CVE-2022-26572**	N/A	O-XER-COLO-190422/901
Vendor: Zyxel					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ax7501-b0_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-AX75-190422/902
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-AX75-190422/903
Product: dx5401-b0_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-DX54-190422/904

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-DX54-190422/905
Product: emg3525-t50b_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-EMG3-190422/906
Buffer Copy without Checking Size of Input	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A	https://www.zyxel.com/support/OS-command-injection-and-buffer-	O-ZYX-EMG3-190422/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	overflow-vulnerabilities-of-CPE-and-ONTs.shtml	
Product: emg5523-t50b_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-EMG5-190422/908
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-EMG5-190422/909
Product: emg5723-t50k_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-EMG5-190422/910
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-EMG5-190422/911
Product: emg6726-b10a_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-EMG6-190422/912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-EMG6-190422/913
Product: ep240p_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-EP24-190422/914
Buffer Copy without Checking Size of Input ('Classic	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-	O-ZYX-EP24-190422/915

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	vulnerabilities-of-CPE-and-ONTs.shtml	
Product: ex3510-b0_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-EX35-190422/916
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-EX35-190422/917
Product: ex5401-b0_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-EX54-190422/918
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-EX54-190422/919
Product: ex5501-b0_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-EX55-190422/920

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-EX55-190422/921
Product: pm7300-t0_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-PM73-190422/922
Buffer Copy without Checking Size of Input ('Classic	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-	O-ZYX-PM73-190422/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	vulnerabilities-of-CPE-and-ONTs.shtml	
Product: pmg5317-t20b_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-PMG5-190422/924
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-PMG5-190422/925
Product: pmg5617-t20b2_firmware					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-PMG5-190422/926
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-PMG5-190422/927
Product: pmg5617ga_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-PMG5-190422/928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-PMG5-190422/929
Product: pmg5622ga_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-PMG5-190422/930
Buffer Copy without Checking Size of Input ('Classic	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-	O-ZYX-PMG5-190422/931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	vulnerabilities-of-CPE-and-ONTs.shtml	
Product: px7501-b0_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-PX75-190422/932
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-PX75-190422/933
Product: vmg1312-t20b_firmware					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG1-190422/934
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG1-190422/935
Product: vmg3312-t20a_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG3-190422/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG3-190422/937
Product: vmg3625-t50b_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG3-190422/938
Buffer Copy without Checking Size of Input ('Classic	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-	O-ZYX-VMG3-190422/939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	vulnerabilities-of-CPE-and-ONTs.shtml	
Product: vmg3927-b50a_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG3-190422/940
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG3-190422/941
Product: vmg3927-b50b_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG3-190422/942
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG3-190422/943
Product: vmg3927-b60a_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG3-190422/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG3-190422/945
Product: vmg3927-t50k_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG3-190422/946
Buffer Copy without Checking Size of Input ('Classic	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-	O-ZYX-VMG3-190422/947

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	vulnerabilities-of-CPE-and-ONTs.shtml	
Product: vmg4927-b50a_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG4-190422/948
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG4-190422/949
Product: vmg8623-t50b_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG8-190422/950
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG8-190422/951
Product: vmg8825-b50a_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG8-190422/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG8-190422/953
Product: vmg8825-b50b_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG8-190422/954
Buffer Copy without Checking Size of Input ('Classic	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-	O-ZYX-VMG8-190422/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	vulnerabilities-of-CPE-and-ONTs.shtml	
Product: vmg8825-b60a_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG8-190422/956
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG8-190422/957
Product: vmg8825-b60b_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG8-190422/958
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG8-190422/959
Product: vmg8825-t50k_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG8-190422/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-VMG8-190422/961
Product: xmg3927-b50a_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-XMG3-190422/962
Buffer Copy without Checking Size of Input ('Classic	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-	O-ZYX-XMG3-190422/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	vulnerabilities-of-CPE-and-ONTs.shtml	
Product: xmg8825-b50a_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Apr-22	8	A command injection vulnerability in the CGI program of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface. **CVE ID : CVE-2022-26413**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-XMG8-190422/964
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Apr-22	5.5	A potential buffer overflow vulnerability was identified in some internal functions of Zyxel VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service. **CVE ID : CVE-2022-26414**	https://www.zyxel.com/support/OS-command-injection-and-buffer-overflow-vulnerabilities-of-CPE-and-ONTs.shtml	O-ZYX-XMG8-190422/965