

National Critical Information Infrastructure Protection Centre Common Vulnerabilities and Exposures (CVE) Report

16 - 28 Feb 2023

Vol. 10 No. 04

Table of Content		
Vendor	Product	Page Number
Application		
add_user_project	add_user	1
	after_effects	1
	animate	5
	bridge	8
Adobe	connect	15
nuobe	framemaker	16
	indesign	20
	photoshop	22
	premiere_rush	27
afl\+\+_project	afl\+\+	28
aioseo	all_in_one_seo	28
alphaware_simple_e- commerce_system_proje ct	alphaware_simple_e-commerce_system	29
answer	answer	30
	airflow_hive_provider	30
	airflow_sqoop_provider	31
	apache-airflow-providers-amazon	31
Apache	apache-airflow-providers-google	31
	commons_fileupload	32
	kerby	33
	sling_i18n	34
api-platform	core	35
apolloconfig	apollo	40
Apple	safari	41
apusthemes	wp_private_messaging	43
artisanworkshop	japanized_for_woocommerce	44

Vendor	Product	Page Number
art_gallery_management _system_project	art_gallery_management_system	45
automatorwp	automatorwp	46
auto_dealer_managemen t_system_project	auto_dealer_management_system	46
axcora	axcora	49
best_pos_management_s ystem_project	best_pos_management_system	49
ВМС	control-m	51
bootstrapped	easy_affiliate_links	51
borg_project	borg	52
bstek	urule	52
btcpayserver	btcpay_server	52
business_management_s ystem_project	business_management_system	53
canteen_management_sy stem_project	canteen_management_system	53
cellinx	nvt_web_server	54
cerebrate-project	cerebrate	54
chamberlain	myq	54
changedetection	changedetection	55
checkoutplugins	stripe_payments_for_woocommerce	55
	application_policy_infrastructure_controller	56
Cisco	cloud_network_controller	58
	node-jose	59
	ucs_central_software	60
Citrix	virtual_apps_and_desktops	65
	workspace	66
clash_project	clash	68
class_and_exam_timetabl ing_system_project	class_and_exam_timetabling_system	69
clinics_patient_managem ent_system_project	clinics_patient_management_system	69
correos	correos_oficial	70

Vendor	Product	Page Number
covesa	dlt-daemon	71
Craftercms	crafter_cms	71
crasm_project	crasm	72
dataease	dataease	73
davinci_project	davinci	73
Dell	multifunction_printer_e525w_driver_and_soft ware_suite	74
	secure_connect_gateway	74
deltaww	diaenergie	75
deno	deno	75
dental_clinic_appointme nt_reservation_system_p roject	dental_clinic_appointment_reservation_system	76
devowl	real_media_library	77
docmosis	tornado	78
doctors_appointment_sy stem_project	doctors_appointment_system	79
dolphinphp_project	dolphinphp	83
domoticalabs	ikon_server	84
donation_block_for_payp al_project	donation_block_for_paypal	84
ecisp	espcms	85
embedsocial	embedsocial	85
embeusociai	embedstories	86
employee_task_manage ment_system_project	employee_task_management_system	86
eternal_terminal_project	eternal_terminal	88
executablebooks	markdown-it-py	88
Filseclab	twister_antivirus	89
Flatpress	flatpress	91
Forgorock	java_policy_agents	91
Forgerock	web_policy_agents	92
Fortinet	fortinac	92
rorunet	fortiweb	97

Vendor	Product	Page Number
frappant	forms_export	114
Froxlor	froxlor	115
GE	digital_industrial_gateway_server	116
Genetechsolutions	pie_register	116
Gentoo	soko	117
geotools	geotools	119
Github	enterprise_server	123
Gluster	glusterfs	123
Gnome	epiphany	124
gnpublisher	gn_publisher	124
GNU	libmicrohttpd	125
go-redrock	tutortrac	125
Google	chrome	126
gpac	gpac	129
gradio_project	gradio	129
greenshiftwp	greenshift _animation_and_page_builder_blocks	130
	gs_books_showcase	131
	gs_filterable_portfolio	131
gsplugins	gs_insever_portfolio	132
	gs_portfolio_for_envato	132
	gs_products_slider	133
hashicorp	go-getter	133
nasincorp	nomad	134
hasthemes	extensions_for_cf7	135
nastnemes	shoplentor	135
Нахх	curl	136
hour_of_code_python_20 15_project	hour_of_code_python_2015	139
	aspera_faspex	139
IBM	cloud_pak_for_business_automation	140
	infosphere_information_server	146
jd-gui_project	jd-gui	148

Vendor	Product	Page Number
Joomla	joomla\!	148
joomunited	wp_meta_seo	148
judging_management_sy stem_project	judging_management_system	153
kainelabs	youzify	154
kavitareader	kavita	154
	arigato_autoresponder_and_newsletter	155
Kibokolabs	namaste\!_lms	155
	watu_quiz	156
krontech	single_connect	157
laravel-admin	laravel-admin	157
Libreswan	libreswan	157
Linuxfoundation	argo-cd	158
Linuxioundation	containerd	163
lite-web-server_project	lite-web-server	167
loan_comparison_project	loan_comparison	168
luckyframe	luckyframeweb	168
mainwp	motomo	169
Mantisbt	mantisbt	169
markdown- electron_project	markdown-electron	170
marktext	marktext	171
mattermost	mattermost	171
mattermost	mattermost_server	174
media_library_assistant_ project	media_library_assistant	175
medical_certificate_gene rator_app_project	medical_certificate_generator_app	175
Microweber	microweber	176
minio	minio	176
misskey	misskey	177
madahaa	installer	180
modoboa	modoboa	180

Vendor	Product	Page Number
mod_gnutls_project	mod_gnutls	181
Mono-project	mono	182
Moodle	moodle	182
moosikay_e- commerce_system_proje ct	moosikay_e-commerce_system	188
music_gallery_site_proje ct	music_gallery_site	188
muyucms	muyucms	192
mz-automation	lib60870	195
Neo4j	awesome_procedures_on_cyper	195
nethack	nethack	197
netmodule	netmodule_router_software	197
networktocode	nautobot	202
Nextcloud	nextcloud_server	206
Nextciouu	nextcloud_talk	213
nic	knot_resolver	213
Nodejs	node.js	214
Nouejs	undici	226
notation-go_project	notation-go	227
notepadproject	notepad	230
nuxt	nuxt	230
olevmedia	olevmedia_shortcodes	231
online_boat_reservation_ system_project	online_boat_reservation_system	231
online_catering_reservat ion_system_project	online_catering_reservation_system	232
online_eyewear_shop_pr oject	online_eyewear_shop	233
online_graduate_tracer_s ystem_project	online_graduate_tracer_system	234
online_pet_shop_we_app_ project	online_pet_shop_we_app	234
online_pizza_ordering_sy stem_project	online_pizza_ordering_system	235

Vendor	Product	Page Number
online_reviewer_manage ment_system_project	online_reviewer_management_system	238
online_services_project	online_services	239
online_student_manage ment_system_project	online_student_management_system	240
Open-emr	openemr	241
opencats	opencats	242
Opennms	horizon	243
opennins	meridian	247
osgeo	geonode	250
03600	geoserver	250
part-db_project	part-db	256
peazip_project	peazip	257
pharmacy_management_ system_project	pharmacy_management_system	257
РНР	php	258
php-saml-sp_project	php-saml-sp	261
Phpmyfaq	phpmyfaq	262
Pimcore	pimcore	262
pixelfed	pixelfed	262
premio	my_sticky_elements	263
	kepware_server	264
	kepware_serverex	264
	thingworxnet-sdk	265
РТС	thingworx_edge_c-sdk	265
	thingworx_edge_microserver	266
	thingworx_industrial_connectivity	267
	thingworx_kepware_edge	267
puzzle	liima	268
Python	python	269
quantumcloud	chatbot	269
quarkus	quarkus	269
quick-plugins	loan_comparison	270

Vendor	Product	Page Number
rangy_project	rangy	271
read_more_excerpt_link_ project	read_more_excerpt_link	271
realtimelogic	fuguhub	272
	build_of_quarkus	272
Redhat	directory_server	273
	resteasy	275
rocket.chat	rocket.chat	276
Rockwellautomation	kepserver_enterprise	276
rosariosis	rosariosis	277
salesagility	suitecrm	277
sales_tracker_manageme nt_system_project	sales_tracker_management_system	278
sandhillsdev	easy_digital_downloads	279
	clearscada	280
Schneider-electric	ecostruxure_geo_scada_expert_2019	281
Schneider-electric	ecostruxure_geo_scada_expert_2020	299
	ecostruxure_geo_scada_expert_2021	314
seacms	seacms	320
sequelizejs	sequelize	320
shortpixel	shortpixel_adaptive_images	322
simple_customer_relatio nship_management_syst em_project	simple_customer_relationship_management_s ystem	323
simple_food_ordering_sy stem_project	simple_food_ordering_system	325
simple_responsive_touri sm_website_project	simple_responsive_tourism_website	326
smeup	erp	327
smg-webdesign	shortcode_for_font_awesome	328
snyk	kubernetes_monitor	328
Spip	spip	329
ss-proj	shirasagi	331
stagil	stagil_navigation	332

Vendor	Product	Page Number
strategy11	formidable_form_builder	333
struktur	libheif	333
sudo_project	sudo	334
Teampass	teampass	334
tachnawarun	dram_calculator_for_ryzen	334
techpowerup	realtemp	335
tftpd64_project	tftpd64	336
themekraft	buddyforms	336
thingsboard	thingsboard	337
Tibco	businessconnect	337
timed_content_project	timed_content	338
tri	gigpress	338
trustedcomputinggroup	trusted_platform_module	339
typecho	typecho	340
ujcms	ujcms	340
uptime-kuma_project	uptime-kuma	341
utilities_project	utilities	341
vektor-inc	vk_all_in_one_expansion_unit	342
versionn_project	versionn	342
	carbon_black_app_control	343
Vmware	vrealize_automation	344
Villwale	vrealize_orchestrator	345
	workspace_one_content	345
vox2png_project	vox2png	346
wangeditor	wangeditor	346
weintek	easybuilder_pro	347
wow-company	wp_coder	347
	booking_calendar	348
wpdevart	organization_chart	349
	responsive_vertical_icon_menu	349
wpdeveloper	reviewx	349
wpgeodirectory	geodirectory	350

Vendor	Product	Page Number
wp_font_awesome_proje ct	wp_font_awesome	350
xoslab	easy_file_locker	351
yoga_class_registration_s ystem_project	yoga_class_registration_system	351
zetacomponenets	mvctools	353
Zoneminder	Zoneminder	353
Hardware		
abus	tvip_20000-21150	364
Axis	207w	365
	firepower_4100	365
	firepower_4110	367
	firepower_4112	369
	firepower_4115	372
	firepower_4120	374
	firepower_4125	376
	firepower_4140	378
	firepower_4145	380
	firepower_4150	383
	firepower_9300_sm-24	385
Circo	firepower_9300_sm-36	387
Cisco	firepower_9300_sm-40	389
	firepower_9300_sm-44	391
	firepower_9300_sm-44_x_3	393
	firepower_9300_sm-48	396
	firepower_9300_sm-56	398
	firepower_9300_sm-56_x_3	400
	mds_9000	402
	mds_9100	403
	mds_9132t	404
	mds_9134	405
	mds_9140	406
	mds_9148	407

Vendor	Product	Page Number
	mds_9148s	407
	mds_9148t	408
	mds_9200	409
	mds_9216	410
	mds_9216a	411
	mds_9216i	412
	mds_9222i	412
	mds_9250i	413
	mds_9396s	414
	mds_9396t	415
	mds_9500	416
	mds_9506	417
	mds_9509	418
	mds_9513	418
	mds_9700	419
Cisco	mds_9706	420
CISCO	mds_9710	421
	mds_9718	422
	nexus_1000v	423
	nexus_1000_virtual_edge	423
	nexus_3016	424
	nexus_3016q	425
	nexus_3048	426
	nexus_3064	427
	nexus_3064-32t	428
	nexus_3064-t	429
	nexus_3064-x	429
	nexus_3064t	430
	nexus_3064x	431
	nexus_3100	432
	nexus_3100-v	433
	nexus_3100-z	434

Vendor	Product	Page Number
	nexus_3100v	435
	nexus_31108pc-v	435
	nexus_31108pv-v	436
	nexus_31108tc-v	437
	nexus_31128pq	438
	nexus_3132c-z	439
	nexus_3132q	440
	nexus_3132q-v	440
	nexus_3132q-x	441
	nexus_3132q-xl	442
	nexus_3132q-x\/3132q-xl	443
	nexus_3164q	444
	nexus_3172	445
	nexus_3172pq	446
	nexus_3172pq-xl	446
Cisco	nexus_3172pq\/pq-xl	447
CISCO	nexus_3172tq	448
	nexus_3172tq-32t	449
	nexus_3172tq-xl	450
	nexus_3200	451
	nexus_3232c	452
	nexus_3232c_	452
	nexus_3264c-e	453
	nexus_3264q	454
	nexus_3400	455
	nexus_3408-s	456
	nexus_34180yc	457
	nexus_34200yc-sm	457
	nexus_3432d-s	458
	nexus_3464c	459
	nexus_3500	460
	nexus_3524	461

Vendor	Product	Page Number
	nexus_3524-x	462
	nexus_3524-xl	463
	nexus_3524-x\/xl	463
	nexus_3548	464
	nexus_3548-x	465
	nexus_3548-xl	466
	nexus_3548-x\/xl	467
	nexus_3600	468
	nexus_36180yc-r	469
	nexus_3636c-r	469
	nexus_5500	470
	nexus_5548p	471
	nexus_5548up	472
	nexus_5596t	473
	nexus_5596up	474
Cisco	nexus_5600	474
CISCO	nexus_56128p	475
	nexus_5624q	476
	nexus_5648q	477
	nexus_5672up	478
	nexus_5672up-16g	479
	nexus_5696q	480
	nexus_6000	480
	nexus_6001	481
	nexus_6001p	482
	nexus_6001t	483
	nexus_6004	484
	nexus_6004x	485
	nexus_7000	486
	nexus_7004	486
	nexus_7009	487
	nexus_7010	488

Vendor	Product	Page Number
	nexus_7018	489
	nexus_7700	490
	nexus_7702	491
	nexus_7706	491
	nexus_7710	492
	nexus_7718	493
	nexus_9000	494
	nexus_9000v	495
	nexus_92160yc-x	497
	nexus_92300yc	498
	nexus_92304qc	500
	nexus_92348gc-x	501
	nexus_9236c	503
	nexus_9272q	504
	nexus_93108tc-ex	505
Cisco	nexus_93108tc-ex-24	507
CISCO	nexus_93108tc-fx	508
	nexus_93108tc-fx-24	510
	nexus_93108tc-fx3p	511
	nexus_93120tx	512
	nexus_93128tx	514
	nexus_9316d-gx	515
	nexus_93180lc-ex	517
	nexus_93180yc-ex	518
	nexus_93180yc-ex-24	519
	nexus_93180yc-fx	521
	nexus_93180yc-fx-24	522
	nexus_93180yc-fx3	523
	nexus_93180yc-fx3s	526
	nexus_93216tc-fx2	528
	nexus_93240yc-fx2	529
	nexus_9332c	531

Vendor	Product	Page Number
	nexus_9332d-gx2b	532
	nexus_9332pq	534
	nexus_93360yc-fx2	535
	nexus_9336c-fx2	536
	nexus_9336c-fx2-e	538
	nexus_9336pq_aci_spine	539
	nexus_9348d-gx2a	541
	nexus_9348gc-fxp	542
	nexus_93600cd-gx	543
	nexus_9364c	545
	nexus_9364c-gx	546
	nexus_9364d-gx2a	548
	nexus_9372px	549
	nexus_9372px-e	550
	nexus_9372tx	552
Cisco	nexus_9372tx-e	553
	nexus_9396px	554
	nexus_9396tx	556
	nexus_9408	557
	nexus_9508	559
	nexus_9808	560
	ucs_6200	561
	ucs_6248up	564
	ucs_6296up	566
	ucs_6300	568
	ucs_6324	570
	ucs_6332	572
	ucs_6332-16up	574
	ucs_64108	577
	ucs_6454	580
	ucs_6536	583
Dell	a200	586

Vendor	Product	Page Number
	a2000	587
	f800	587
	f810	588
Dell	h400	588
	h500	589
	h5600	590
	h600	590
Draytek	vigor2960	591
НЗС	a210-g	592
	jetwave_2111	592
	jetwave_2111l	593
	jetwave_2114	594
	jetwave_2211c	595
	jetwave_2212g	596
	jetwave_2212s	597
Korenix	jetwave_2212x	598
Koremix	jetwave_2411	599
	jetwave_2411l	599
	jetwave_2414	600
	jetwave_2460	601
	jetwave_3220_v3	602
	jetwave_3420_v3	603
	jetwave_4221hp-e	604
	fx0-gent00000	605
sick	fx0-gent00010	606
SICK	fx0-gpnt00000	606
	fx0-gpnt00010	607
	ac500	607
	ax3	608
Tenda	ср3	608
	cp7	609
	it7-lcs	609

Vendor	Product	Page Number
	it7-pcs	610
Tenda	it7-prs	610
	w30e	611
totolink	a7100ru	611
totomik	a720r	612
Tp-link	archer_c50	612
i p-mik	tl-wr940n	613
ui	unifi_dream_machine_pro	613
Zyxel	lte3202-m437	614
Lyxei	lte3316-m604	614
Operating System		
abus	tvip_20000-21150_firmware	615
	ipados	615
	iphone_os	628
Apple	macos	640
	tvos	673
	watchos	680
Asus	asmb8-ikvm_firmware	687
Axis	207w_firmware	688
	fxos	688
	nexus_93180yc-fx3s_firmware	690
	nexus_93180yc-fx3_firmware	691
	nx-os	692
	ucs_6200_firmware	717
	ucs_6248up_firmware	719
Cisco	ucs_6296up_firmware	722
	ucs_6300_firmware	724
	ucs_6324_firmware	726
	ucs_6332-16up_firmware	728
	ucs_6332_firmware	730
	ucs_64108_firmware	733
	ucs_6454_firmware	736

Vendor	Product	Page Number
Cisco	ucs_6536_firmware	739
Debian	debian_linux	742
	a2000_firmware	745
	a200_firmware	749
	emc_powerscale_onefs	754
	f800_firmware	754
Dell	f810_firmware	758
	h400_firmware	762
	h500_firmware	767
	h5600_firmware	771
	h600_firmware	775
Draytek	vigor2960_firmware	779
Fedoraproject	fedora	780
Google	android	783
НЗС	a210-g_firmware	804
IBM	aix	804
	jetwave_2111l_firmware	805
	jetwave_2111_firmware	806
	jetwave_2114_firmware	807
	jetwave_2211c_firmware	808
	jetwave_2212g_firmware	809
	jetwave_2212s_firmware	810
	jetwave_2212x_firmware	811
Korenix	jetwave_2411l_firmware	812
	jetwave_2411_firmware	813
	jetwave_2414_firmware	813
	jetwave_2424_firmware	814
	jetwave_2460_firmware	815
	jetwave_3220_v3_firmware	816
	jetwave_3420_v3_firmware	817
	jetwave_4221hp-e_firmware	818
Linux	linux_kernel	819

Vendor	Product	Page Number
Microsoft	windows	829
Redhat	enterprise_linux	846
	fx0-gent00000_firmware	847
sick	fx0-gent00010_firmware	848
SICK	fx0-gpnt00000_firmware	849
	fx0-gpnt00010_firmware	850
	ac500_firmware	851
	ax3_firmware	852
	cp3_firmware	852
Tenda	cp7_firmware	853
Tenua	it7-lcs_firmware	853
	it7-pcs_firmware	854
	it7-prs_firmware	854
	w30e_firmware	855
totolink	a7100ru_firmware	855
totomik	a720r_firmware	856
Tn link	archer_c50	856
Tp-link	tl-wr940n_firmware	857
ui	unifi_dream_machine_pro_firmware	857
7.00	lte3202-m437_firmware	858
Zyxel	lte3316-m604_firmware	858

Common Vulnerabilities and Exposures (CVE) Report					
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
	I	1	Application	l	
Vendor: add	d_user_project				
Product: ad	d_user				
Affected Ver	sion(s): * Up to	(including	g) 2.0.2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	6.1	The Custom Add User WordPress plugin through 2.0.2 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	N/A	A-ADD-ADD 160323/1
Vendor: Ad	obe		CVE ID : CVE-2023- 0043		
Product: aft	er_effects				
Affected Ver	sion(s): From (i	ncluding)	22.0.0 Up to (excluding	;) 22.6.4	
Out-of- bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/after_effect s/apsb23- 02.html	A-ADO-AFTE- 160323/2

0-1

1-2

2-3

3-4 4-5 Page **1** of **859** 6-7

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22237		
Out-of- bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22238	https://helpx. adobe.com/se curity/produc ts/after_effect s/apsb23- 02.html	A-ADO-AFTE- 160323/3
Improper Input Validation	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22239	https://helpx. adobe.com/se curity/produc ts/after_effect s/apsb23- 02.html	A-ADO-AFTE- 160323/4
Out-of- bounds Read	17-Feb-2023	5.5	After Affects versions 23.1 (and earlier), 22.6.3 (and	https://helpx. adobe.com/se curity/produc	A-ADO-AFTE- 160323/5

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22233	ts/after_effect s/apsb23- 02.html	
Affected Ver	sion(s): From (i	ncluding)	23.0.0 Up to (excluding) 23.2.0	
Out-of- bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22237	https://helpx. adobe.com/se curity/produc ts/after_effect s/apsb23- 02.html	A-ADO-AFTE- 160323/6
Out-of- bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds	https://helpx. adobe.com/se curity/produc ts/after_effect	A-ADO-AFTE- 160323/7

0-1

1-2

2-3

3-4 4-5 Page **3** of **859** 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22238	s/apsb23- 02.html	
Improper Input Validation	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22239	https://helpx. adobe.com/se curity/produc ts/after_effect s/apsb23- 02.html	A-ADO-AFTE- 160323/8
Out-of- bounds Read	17-Feb-2023	5.5	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	https://helpx. adobe.com/se curity/produc ts/after_effect s/apsb23- 02.html	A-ADO-AFTE- 160323/9

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22233		
Product: an	imate				
Affected Ver	sion(s): 23.0.0				
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Heap- based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22236	https://helpx. adobe.com/se curity/produc ts/animate/ap sb23-15.html	A-ADO-ANIM- 160323/10
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Stack- based Buffer Overflow vulnerability that could result in arbitrary code	https://helpx. adobe.com/se curity/produc ts/animate/ap sb23-15.html	A-ADO-ANIM- 160323/11

0-1

1-2

2-3

3-4 4-5 Page **5** of **859** 6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22243		
Use After Free	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22246	https://helpx. adobe.com/se curity/produc ts/animate/ap sb23-15.html	A-ADO-ANIM- 160323/12
Affected Ver	<mark>sion(s): From (</mark> i	ncluding)	22.0.0 Up to (including) 22.0.8	
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Heap- based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the	https://helpx. adobe.com/se curity/produc ts/animate/ap sb23-15.html	A-ADO-ANIM- 160323/13

0-1

1-2

2-3

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2023- 22236		
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Stack- based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-	https://helpx. adobe.com/se curity/produc ts/animate/ap sb23-15.html	A-ADO-ANIM- 160323/14
Use After Free	17-Feb-2023	7.8	22243 Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx. adobe.com/se curity/produc ts/animate/ap sb23-15.html	A-ADO-ANIM- 160323/15

0-1

1-2

2-3

3-4 4-5 Page **7** of **859** 5-6

6-7 7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file.		
			CVE ID : CVE-2023- 22246		
Product: br	idge				
Affected Ver	sion(s): From (i	ncluding)	12.0.0 Up to (excluding) 12.0.4	
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by a Stack- based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22226	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	A-ADO-BRID- 160323/16
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	A-ADO-BRID- 160323/17

0-1

1-2

2-3

3-4 4-5 Page **8** of **859** 5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file.		
			CVE ID : CVE-2023- 22227		
Improper Input Validation	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22228	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	A-ADO-BRID- 160323/18
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	A-ADO-BRID- 160323/19

0-1

1-2

2-3

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22229		
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22230	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	A-ADO-BRID- 160323/20
Out-of- bounds Read	17-Feb-2023	5.5	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	A-ADO-BRID- 160323/21

0-1

1-2

2-3

3-4 4-5 Page **10** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21583		
Out-of- bounds Read	17-Feb-2023	5.5	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22231	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	A-ADO-BRID- 160323/22
Affected ver	sion(s): From (i	nciuaingj	13.0.0 Up to (excluding	J 13.0.2	
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by a Stack- based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	A-ADO-BRID- 160323/23

0-1

1-2

2-3

3-4 4-5 Page **11** of **859** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. CVE ID : CVE-2023-		
			22226		
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22227	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	A-ADO-BRID- 160323/24
Improper Input Validation	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	A-ADO-BRID- 160323/25

0-1

1-2

2-3

3-4 4-5 Page **12** of **859** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22228		
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22229	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	A-ADO-BRID- 160323/26
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22230	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	A-ADO-BRID- 160323/27

0-1

1-2

2-3

3-4 4-5

8-9 7-8

9-10

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	17-Feb-2023	5.5	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21583	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	A-ADO-BRID- 160323/28
Out-of- bounds Read	17-Feb-2023	5.5	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	A-ADO-BRID- 160323/29

0-1

1-2

2-3

3-4 4-5 Page **14** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22231		
Product: co	nnect				
Affected Ver	sion(s): From (i	ncluding)	11.0 Up to (including)	11.4.5	-
N/A	17-Feb-2023	5.3	Adobe Connect versions 11.4.5 (and earlier), 12.1.5 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to impact the integrity of a minor feature. Exploitation of this issue does not require user interaction. CVE ID : CVE-2023- 22232	https://helpx. adobe.com/se curity/produc ts/connect/ap sb23-05.html	A-ADO-CONN- 160323/30
Affected Ver	sion(s): From (i	ncluding)	12.0 Up to (including)	12.1.5	
N/A	17-Feb-2023	5.3	Adobe Connect versions 11.4.5 (and earlier), 12.1.5 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to impact the integrity of a minor feature. Exploitation of this issue does not	https://helpx. adobe.com/se curity/produc ts/connect/ap sb23-05.html	A-ADO-CONN- 160323/31

0-1

1-2

2-3

3-4 4-5 Page **15** of **859** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			require user interaction. CVE ID : CVE-2023-						
			22232						
	Product: framemaker Affected Version(s): * Up to (including) 2020.0.4								
Affected ver	sion(s): • Op to	(including	FrameMaker 2020						
Out-of- bounds Write	17-Feb-2023	7.8	Update 4 (and earlier), 2022 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-	https://helpx. adobe.com/se curity/produc ts/framemake r/apsb23- 06.html	A-ADO-FRAM- 160323/32				
Improper Input Validation	17-Feb-2023	7.8	21619 FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/framemake r/apsb23- 06.html	A-ADO-FRAM- 160323/33				

0-1

1-2

2-3

3-4 4-5 Page **16** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21621		
Out-of- bounds Write	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21622	https://helpx. adobe.com/se curity/produc ts/framemake r/apsb23- 06.html	A-ADO-FRAM- 160323/34
Use After Free	17-Feb-2023	5.5	FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21584	https://helpx. adobe.com/se curity/produc ts/framemake r/apsb23- 06.html	A-ADO-FRAM- 160323/35

0-1

1-2

2-3

3-4 4-5 Page **17** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	17-Feb-2023	5.5	FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21620	https://helpx. adobe.com/se curity/produc ts/framemake r/apsb23- 06.html	A-ADO-FRAM- 160323/36
Affected Ver	sion(s): 2022				_
Out-of- bounds Write	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21619	https://helpx. adobe.com/se curity/produc ts/framemake r/apsb23- 06.html	A-ADO-FRAM- 160323/37

0-1

1-2

2-3

3-4 4-5 Page **18** of **859** 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21621	https://helpx. adobe.com/se curity/produc ts/framemake r/apsb23- 06.html	A-ADO-FRAM- 160323/38
Out-of- bounds Write	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21622	https://helpx. adobe.com/se curity/produc ts/framemake r/apsb23- 06.html	A-ADO-FRAM- 160323/39
Use After Free	17-Feb-2023	5.5	FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by a Use After Free vulnerability that	https://helpx. adobe.com/se curity/produc ts/framemake	A-ADO-FRAM- 160323/40

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21584	r/apsb23- 06.html	
Out-of- bounds Read	17-Feb-2023	5.5	FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21620	https://helpx. adobe.com/se curity/produc ts/framemake r/apsb23- 06.html	A-ADO-FRAM- 160323/41
Product: inc	-				
Affected Vers	sion(s): 18.0				
NULL Pointer Dereferenc e	17-Feb-2023	5.5	Adobe InDesign versions ID18.1 (and earlier) and ID17.4 (and earlier) are	https://helpx. adobe.com/se curity/produc ts/indesign/a	A-ADO-INDE- 160323/42
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3 3-4 4-5 5</mark> Page 20 of 859	-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of- service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-	psb23- 12.html	
Affected Ver	sion(s): 18.1		21593		
NULL Pointer Dereferenc e	17-Feb-2023	5.5	Adobe InDesign versions ID18.1 (and earlier) and ID17.4 (and earlier) are affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of- service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21593	https://helpx. adobe.com/se curity/produc ts/indesign/a psb23- 12.html	A-ADO-INDE- 160323/43

0-1

1-2

2-3

3-4 4-5 Page **21** of **859** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereferenc e	17-Feb-2023	5.5	Adobe InDesign versions ID18.1 (and earlier) and ID17.4 (and earlier) are affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of- service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21593	https://helpx. adobe.com/se curity/produc ts/indesign/a psb23- 12.html	A-ADO-INDE- 160323/44
Product: ph		<u> </u>			
Affected Ver	sion(s): From (i	ncluding)	23.0.0 Up to (excluding) 23.5.4	
Improper Input Validation	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	A-ADO-PHOT- 160323/45

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21574		
Out-of- bounds Write	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21575	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	A-ADO-PHOT- 160323/46
Out-of- bounds Write	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21576	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	A-ADO-PHOT- 160323/47
Out-of- bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of-	https://helpx. adobe.com/se curity/produc ts/photoshop	A-ADO-PHOT- 160323/48

0-1

1-2

3-4 4-5 Page **23** of **859** 5-6

6-7

7-8

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21577	/apsb23- 11.html	
Out-of- bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of- bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21578	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	A-ADO-PHOT- 160323/49
Affected Ver	 <mark>sion(s): From (</mark> i	ncluding)	24.0.0 Up to (excluding) 24.1.1	
Improper Input Validation	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are	https://helpx. adobe.com/se curity/produc	A-ADO-PHOT- 160323/50

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

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-	ts/photoshop /apsb23- 11.html	
Out-of- bounds Write	17-Feb-2023	7.8	21574 Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21575	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	A-ADO-PHOT- 160323/51
Out-of- bounds Write	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	A-ADO-PHOT- 160323/52

0-1

1-2

2-3

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21576		
Out-of- bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of- bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21577	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	A-ADO-PHOT- 160323/53
Out-of- bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of- bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	A-ADO-PHOT- 160323/54

0-1

1-2

2-3

6-7

7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2023- 21578		
Product: pr	emiere_rush				
Affected Ver	sion(s): * Up to	(including			
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Premiere Rush version 2.6 (and earlier) is affected by a Stack- based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22234	https://helpx. adobe.com/se curity/produc ts/premiere_r ush/apsb23- 14.html	A-ADO-PREM- 160323/55
Use After Free	17-Feb-2023	7.8	Adobe Premiere Rush version 2.6 (and earlier) is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user	https://helpx. adobe.com/se curity/produc ts/premiere_r ush/apsb23- 14.html	A-ADO-PREM- 160323/56

0-1

1-2

2-3

3-4 4-5 Page **27** of **859** 5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2023- 22244		
Vendor: afl	+\+_project				
Product: afl					
Affected Vers	sion(s): 4.05c			1	
N/A	21-Feb-2023	9.8	In AFL++ 4.05c, the CmpLog component uses the current working directory to resolve and execute unprefixed fuzzing targets, allowing code execution.	https://github .com/AFLplus plus/AFLplus plus/pull/164 3	A-AFL-AFL\- 160323/57
			CVE ID : CVE-2023- 26266		
Vendor: aio					
Product: all					
Affected Vers	sion(s): * Up to	(includinន្		I	Γ
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	24-Feb-2023	5.4	The All in One SEO Pack plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters in versions up to, and including, 4.2.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with Contributor+ role to inject arbitrary web scripts in pages that will execute whenever a user	N/A	A-AIO-ALL 160323/58
	cale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10

Page 28 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accesses an injected page. CVE ID : CVE-2023- 0586		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	24-Feb-2023	4.8	The All in One SEO Pack plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters in versions up to, and including, 4.2.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with Administrator role or above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID : CVE-2023- 0585	N/A	A-AIO-ALL 160323/59
Vendor: alp	haware_simple	e_e-comn	nerce_system_project		
Product: alp	ohaware_simp	e_e-com	nerce_system		
Affected Ver	sion(s): 1.0				
Improper Access Control	24-Feb-2023	5.3	A vulnerability classified as critical has been found in SourceCodester Alphaware Simple E- Commerce System 1.0. This affects an unknown part of the file /alphaware/summar y.php of the	N/A	A-ALP-ALPH- 160323/60
CV/SS Searing (1_2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-6	
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10

Page 29 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component Payment Handler. The manipulation of the argument amount leads to improper access controls. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221733 was assigned to this vulnerability.		
			CVE ID : CVE-2023- 0998		
Vendor: ans	swer			l	
Product: an					
Affected Ver	sion(s): * Up to	(excluding	g) 1.0.5		1
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.5. CVE ID : CVE-2023- 0934	https://huntr. dev/bounties/ cd213098- 5bab-487f- 82c7- 13698ad43b5 1, https://github .com/answerd ev/answer/co mmit/edc069 42d51fa8e56a 134c5c7e5c88 26d9260da0	A-ANS-ANSW- 160323/61
Vendor: Apa					
	flow_hive_pro				
Affected Ver	sion(s): * Up to	(excluding			
Improper Input Validation	24-Feb-2023	9.8	Improper Input Validation vulnerability in the Apache Airflow Hive	https://github .com/apache/ airflow/pull/2 9502,	A-APA-AIRF- 160323/62
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	<u>8 8-9 9-10</u>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Provider. This issue affects Apache Airflow Hive Provider versions before 5.1.3. CVE ID : CVE-2023-	https://lists.a pache.org/thr ead/99g0qm5 6wmgdxmbtd svhj4rdnxhpz pml	
			25696		
Product: air	flow_sqoop_pr	ovider			
Affected Vers	sion(s): * Up to	(excludin	g) 3.1.1	-	-
Improper Input Validation	24-Feb-2023	9.8	Improper Input Validation vulnerability in the Apache Airflow Sqoop Provider. This issue affects Apache Airflow Sqoop Provider versions before 3.1.1.	https://lists.a pache.org/thr ead/79qn8g5 xbq036f8crb1 15obvr22l52q 4, https://github .com/apache/ airflow/pull/2	A-APA-AIRF- 160323/63
			CVE ID : CVE-2023- 25693	9500	
Product: ap	ache-airflow-p	roviders	-amazon		
Affected Vers	sion(s): * Up to	(excludin	g) 7.2.1		
Generation of Error Message Containing Sensitive Informatio n	24-Feb-2023	7.5	Generation of Error Message Containing Sensitive Information vulnerability in the Apache Airflow AWS Provider. This issue affects Apache Airflow AWS Provider versions before 7.2.1. CVE ID : CVE-2023- 25956	https://lists.a pache.org/thr ead/07pl9y4g dpw2c6rzqm7 7dvkm2z2kb5 gv, https://github .com/apache/ airflow/pull/2 9587	A-APA-APAC- 160323/64
Product: ap	ache-airflow-p	roviders			
	sion(s): * Up to				
Improper Input Validation	24-Feb-2023	9.8	Improper Input Validation vulnerability in the	https://lists.a pache.org/thr ead/zdr8ovftt	A-APA-APAC- 160323/65
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3 3-4 4-5 5</mark> Page 31 of 859	-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Apache Airflow Google Provider. This issue affects Apache Airflow Google Provider versions before 8.10.0.	bh7kj0lydgcw 88tbt2nmkcy, https://github .com/apache/ airflow/pull/2 9497	
			CVE ID : CVE-2023- 25691		
Improper Input Validation	24-Feb-2023	7.5	Improper Input Validation vulnerability in the Apache Airflow Google Provider. This issue affects Apache Airflow Google Provider versions before 8.10.0. CVE ID : CVE-2023- 25692	https://lists.a pache.org/thr ead/ks4l78l5r wdpmvfn7y7y hs179nyxtlsh, https://github .com/apache/ airflow/pull/2 9499	A-APA-APAC- 160323/66
Product: co	mmons_fileup	oad			
Affected Ver	sion(s): 1.0		-	-	-
Allocation of Resources Without Limits or Throttling	20-Feb-2023	7.5	Apache Commons FileUpload before 1.5 does not limit the number of request parts to be processed resulting in the possibility of an attacker triggering a DoS with a malicious upload or series of uploads. Note that, like all of the file upload limits, the new configuration option (FileUploadBase#set FileCountMax) is not enabled by default	https://lists.a pache.org/thr ead/4xl4l09m hwg4vgsk7dx qogcjrobrrdoy	A-APA-COMM- 160323/67

0-1

1-2

2-3

3-4 4-5 Page **32** of **859** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and must be explicitly configured. CVE ID : CVE-2023-		
			24998		
Affected Ver	<mark>sion(s): From (</mark> i	ncluding)	1.0 Up to (excluding) 1.	5	
Allocation of Resources Without Limits or Throttling	20-Feb-2023	7.5	Apache Commons FileUpload before 1.5 does not limit the number of request parts to be processed resulting in the possibility of an attacker triggering a DoS with a malicious upload or series of uploads. Note that, like all of the file upload limits, the new configuration option (FileUploadBase#set FileCountMax) is not enabled by default and must be explicitly configured. CVE ID : CVE-2023- 24998	https://lists.a pache.org/thr ead/4xl4l09m hwg4vgsk7dx qogcjrobrrdoy	A-APA-COMM- 160323/68
Product: ke		<u> </u>			
	sion(s): * Up to	(excluding	gj 2.0.3		
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t	20-Feb-2023	9.8	An LDAP Injection vulnerability exists in the LdapIdentityBacken d of Apache Kerby before 2.0.3. CVE ID : CVE-2023- 25613	N/A	A-APA-KERB- 160323/69

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')					
Product: sli	ng_i18n				
Affected Ver	sion(s): * Up to	(excluding	g) 2.6.2		
N/A	23-Feb-2023	6.5	Privilege Escalation vulnerability in Apache Software Foundation Apache Sling. Any content author is able to create i18n dictionaries in the repository in a location the author has write access to. As these translations are used across the whole product, it allows an author to change any text or dialog in the product. For example an attacker might fool someone by changing the text on a delete button to "Info". This issue affects the i18n module of Apache Sling up to version 2.5.18. Version 2.6.2 and higher limit by default i18m dictionaries to certain paths in the repository (/libs and /apps). Users of the module are advised to update to version 2.6.2 or higher, check the configuration for resource loading and then adjust the	N/A	A-APA-SLIN- 160323/70

0-1

1-2

2-3

3-4 4-5 Page **34** of **859** 5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access permissions for the configured path accordingly.		
			CVE ID : CVE-2023- 25621		
Vendor: api	-platform				
Product: co	re				
Affected Ver	sion(s): From (i	ncluding)	2.6.0 Up to (excluding)	2.7.10	
Incorrect Authorizati on	28-Feb-2023	6.5	API Platform Core is the server component of API Platform: hypermedia and GraphQL APIs. Resource properties secured with the `security` option of the `ApiPlatform\Metad ata\ApiProperty` attribute can be disclosed to unauthorized users. The problem affects most serialization formats, including raw JSON, which is enabled by default when installing API Platform. Custom serialization formats may also be impacted. Only collection endpoints are affected by the issue, item endpoints are not. The JSON-LD format is not affected by the issue. The result of the security rule is only executed for the first item of	https://github .com/api- platform/core /commit/572 3d68369722f eefeb11e4252 8d9580db5dd 0fb, https://github .com/api- platform/core /security/advi sories/GHSA- vr2x-7687- h6qv	A-API-CORE- 160323/71

0-1

1-2

2-3

3-4 4-5 Page **35** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the collection. The result of the rule is then cached and reused for the next items. This bug can leak data to unauthorized users when the rule depends on the value of a property of the item. This bug can also hide properties that should be displayed to authorized users. This issue impacts the 2.7, 3.0 and 3.1 branches. Please upgrade to versions 2.7.10, 3.0.12 or 3.1.3. As a workaround, replace the `cache_key` of the context array of the Serializer inside a custom normalizer that works on objects if the security option of the `ApiPlatform\Metad ata\ApiProperty` attribute is used. CVE ID : CVE-2023-		
Affected Ver	sion(s): From (i	ncluding	25575 3.0.0 Up to (excluding)	3012	
				1	
Incorrect Authorizati on	28-Feb-2023	6.5	API Platform Core is the server component of API Platform: hypermedia and GraphQL APIs. Resource properties secured with the	https://github .com/api- platform/core /commit/572 3d68369722f eefeb11e4252 8d9580db5dd 0fb,	A-API-CORE- 160323/72

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`security` option of	https://github	
			the	.com/api-	
			`ApiPlatform\Metad	platform/core	
			ata\ApiProperty`	/security/advi	
			attribute can be	sories/GHSA-	
			disclosed to	vr2x-7687-	
			unauthorized users.	h6qv	
			The problem affects		
			most serialization		
			formats, including		
			raw JSON, which is		
			enabled by default		
			when installing API		
			Platform. Custom		
			serialization formats		
			may also be		
			impacted. Only		
			collection endpoints		
			are affected by the		
			issue, item endpoints		
			are not. The JSON-LD		
			format is not affected		
			by the issue. The		
			result of the security		
			rule is only executed		
			for the first item of		
			the collection. The		
			result of the rule is		
			then cached and		
			reused for the next		
			items. This bug can		
			leak data to unauthorized users		
			when the rule		
			depends on the value		
			of a property of the		
			item. This bug can		
			also hide properties		
			that should be		
			displayed to		
			authorized users.		
			This issue impacts		
			the 2.7, 3.0 and 3.1		
			branches. Please		
l			Stutienes, i lease		

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade to versions 2.7.10, 3.0.12 or 3.1.3. As a workaround, replace the `cache_key` of the context array of the Serializer inside a custom normalizer that works on objects if the security option of the `ApiPlatform\Metad ata\ApiProperty` attribute is used. CVE ID : CVE-2023- 25575		
Affected Ver	sion(s): From (i	ncluding)	3.1.0 Up to (excluding)	3.1.3	
Incorrect Authorizati on	28-Feb-2023	6.5	API Platform Core is the server component of API Platform: hypermedia and GraphQL APIs. Resource properties secured with the `security` option of the `ApiPlatform\Metad ata\ApiProperty` attribute can be disclosed to unauthorized users. The problem affects most serialization formats, including raw JSON, which is enabled by default when installing API Platform. Custom serialization formats may also be impacted. Only collection endpoints	https://github .com/api- platform/core /commit/572 3d68369722f eefeb11e4252 8d9580db5dd 0fb, https://github .com/api- platform/core /security/advi sories/GHSA- vr2x-7687- h6qv	A-API-CORE- 160323/73

0-1

1-2

2-3

3-4 4-5 Page **38** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are affected by the issue, item endpoints		
			are not. The JSON-LD		
			format is not affected		
			by the issue. The		
			result of the security		
			rule is only executed		
			for the first item of		
			the collection. The		
			result of the rule is		
			then cached and		
			reused for the next		
			items. This bug can leak data to		
			unauthorized users		
			when the rule		
			depends on the value		
			of a property of the		
			item. This bug can		
			also hide properties		
			that should be		
			displayed to		
			authorized users.		
			This issue impacts		
			the 2.7, 3.0 and 3.1		
			branches. Please		
			upgrade to versions		
			2.7.10, 3.0.12 or		
			3.1.3. As a		
			workaround, replace the `cache_key` of the		
			context array of the		
			Serializer inside a		
			custom normalizer		
			that works on		
			objects if the security		
			option of the		
			`ApiPlatform\Metad		
			ata\ApiProperty`		
			attribute is used.		
			CVE ID : CVE-2023-		
			25575		
Vendor: apo	olloconfig				I

0-1

1-2

2-3

5-6

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ollo		L	L	L
sion(s): * Up to	(excluding	g) 2.1.0		
20-Feb-2023	7.5	Apollo is a configuration management system. Prior to version 2.1.0, there are potential security issues if users expose apollo-configservice to the internet, which is not recommended. This is because there is no authentication feature enabled for the built-in eureka service. Malicious hackers may access eureka directly to mock apollo- configservice and apollo-adminservice. Login authentication for eureka was added in version 2.1.0. As a workaround, avoid exposing apollo- configservice to the internet. CVE ID : CVE-2023- 25570	https://github .com/apolloco nfig/apollo/p ull/4663, https://github .com/apolloco nfig/apollo/co mmit/7df79bf 8df6960433e d4ff782a54e3 dfc74632bd	A-APO-APOL- 160323/74
20-Feb-2023	5.7	Apollo is a configuration management system. Prior to version 2.1.0, a low- privileged user can create a special web page. If an authenticated portal	https://github .com/apolloco nfig/apollo/p ull/4664, https://github .com/apolloco nfig/apollo/co mmit/00d968 a7229f809b0	A-APO-APOL- 160323/75
	ollo sion(s): * Up to 20-Feb-2023	ollo sion(s): * Up to (excluding 20-Feb-2023 7.5	ollosion(s): * Up to (excluding) 2.1.0Apollo is a configuration management system. Prior to version 2.1.0, there are potential security issues if users expose apollo-configservice to the internet, which is not recommended. This is because there is no authentication feature enabled for the built-in eureka service. Malicious hackers may access eureka directly to mock apollo- configservice and apollo-adminservice. Login authentication for eureka was added in version 2.1.0. As a workaround, avoid exposing apollo- configservice to the internet.20-Feb-20235.7Apollo is a configuration management system. Prior to version 2.1.0, a low- privileged user can create a special web page. If an	ollosion(s): * Up to (excluding) 2.1.0Apollo is a configuration management system. Prior to version 2.1.0, there are potential security issues if users expose apollo-configservice to the internet, which is not recommended. This is because there is no authentication feature enabled for the built-in eureka service. Malicious hackers may access eureka directly to mock apollo- configservice and apollo-adminservice. Login authentication for eureka was added in version 2.1.0. As a workaround, avoid exposing apollo- configservice to the internet.https://github .com/apolloco nfig/apollo/p ull/4663, https://github .com/apolloco nfig/apollo/p ull/4663, https://github .com/apolloco nfig/apollo/p ull/4663, https://github .com/apolloco nfig/apollo/p ull/4663, https://github .com/apolloco nfig/apollo/p ull/4663, https://github .com/apolloco nfig/apollo/p ull/4664, https://github .com/apolloco nfig/apollo/p ull/4664, https://github .com/apolloco nfig/apollo/p ull/4664, https://github .com/apolloco nfig/apollo/p20-Feb-20235.7Apollo is a configuration management system. Prior to version 2.1.0, a low- prior to version

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page, the page can silently send a request to assign new roles for that user without any confirmation from the Portal admin. Cookie SameSite strategy was set to Lax in version 2.1.0. As a workaround, avoid visiting unknown source pages. CVE ID : CVE-2023- 25569	01a6c2b7c75 0	
Vendor: Ap	ple				
Product: sa	fari				
Affected Ver	sion(s): * Up to	(excluding	g) 16.3		
N/A	27-Feb-2023	8.8	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23496	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599 , https://suppo rt.apple.com/	A-APP-SAFA- 160323/76

0-1

1-2

2-3

3-4 4-5 Page **41** of **859** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en- us/HT213600	
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23517	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	A-APP-SAFA- 160323/77
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Wonterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/	A-APP-SAFA- 160323/78

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23518	en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599				
Access of Resource Using Incompatib le Type ('Type Confusion')	27-Feb-2023	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, Safari 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited CVE ID : CVE-2023- 23529	https://suppo rt.apple.com/ en- us/HT213638 , https://suppo rt.apple.com/ en- us/HT213635 , https://suppo rt.apple.com/ en- us/HT213633	A-APP-SAFA- 160323/79			
Vendor: apu	isthemes							
Product: wp_private_messaging Affected Version(s): * Up to (excluding) 1.0.6								
Attected Vers Authorizati on Bypass Through	21-Feb-2023	4.3	The WP Private Message WordPress plugin (bundled with	N/A	A-APU-WP_P- 160323/80			
CVSS Scoring S	CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 43 of 859							

Page **43** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
User- Controlled Key			the Superio theme as a required plugin) before 1.0.6 does not ensure that private messages to be accessed belong to the user making the requests. This allowing any authenticated users to access private messages belonging to other users by tampering the ID. CVE ID : CVE-2023- 0453		
Vendor: art	isanworkshop		0433		
	panized_for_wo		rce		
· •	sion(s): * Up to				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	6.1	The Japanized For WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in versions up to, and including, 2.5.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	https://plugin s.trac.wordpre ss.org/change set?sfp_email= &sfph_mail=& reponame=&n ew=2868545 %40woocom merce-for- japan%2Ftrun k&old=28630 64%40wooco mmerce-for- japan%2Ftrun k&sfp_email= &sfph_mail=	A-ART-JAPA- 160323/81

0-1

1-2

2-3

3-4 4-5 Page **44** of **859** 6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			CVE ID : CVE-2023- 0942						
Vendor: art	Vendor: art_gallery_management_system_project								
Product: art	Product: art_gallery_management_system								
Affected Vers	sion(s): 1.0								
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	9.8	Art Gallery Management System Project in PHP 1.0 was discovered to contain a SQL injection vulnerability via the username parameter in the Admin Login. CVE ID : CVE-2023- 23155	N/A	A-ART-ART 160323/82				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	9.8	Art Gallery Management System Project in PHP 1.0 was discovered to contain a SQL injection vulnerability via the pid parameter in the single-product page. CVE ID : CVE-2023- 23156	N/A	A-ART-ART 160323/83				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	A stored cross-site scripting (XSS) vulnerability in Art Gallery Management System Project v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the fullname parameter on the enquiry page. CVE ID : CVE-2023- 23157	N/A	A-ART-ART 160323/84				
CVSS Scoring S	icale 0-1	1-2 2		-6 6-7 7-8	3 8-9 9-10				

Page **45** of **859**

Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')27-Feb-20235.4Generation system Project v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the message parameter on the enquiry page. CVE ID : CVE-2023- 23158N/AA-ART-ART 160323/85Vendor: auto-matorwp	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: automatorwp Affected Version(s): * Up to (excluding) 2.5.1 Cross-Site Request Forgery (CSRF) 28-Feb-2023 4.3 Cross-Site Request Forgery (CSRF) N/A A-AUT-AUTO- 160323/86 Vulnerability in AutomatorWP plugin <= 2.5.0 leads to object delete. CVE ID : CVE-2023- 23992 N/A A-AUT-AUTO- 160323/86 Vendor: auto_dealer_management_system_project CVE ID : CVE-2023- 23992 X X Product: auto_dealer_management_system_project X X X Affected Version(s): 1.0 A vulnerability classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. This affects an unknown part of the file /adms/admin/?page =vehicles/view_trans action. The manipulation of the argument id leads to N/A A-AUT-AUTO- 160323/87	Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	scripting (XSS) vulnerability in Art Gallery Management System Project v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the message parameter on the enquiry page. CVE ID : CVE-2023-	N/A	_
Product: automatorwp Affected Version(s): * Up to (excluding) 2.5.1 Cross-Site Request Forgery (CSRF) 28-Feb-2023 4.3 Cross-Site Request Forgery (CSRF) N/A A-AUT-AUTO- 160323/86 Vulnerability in AutomatorWP plugin <= 2.5.0 leads to object delete. CVE ID : CVE-2023- 23992 N/A A-AUT-AUTO- 160323/86 Vendor: auto_dealer_management_system_project CVE ID : CVE-2023- 23992 X X Product: auto_dealer_management_system_project X X X Affected Version(s): 1.0 A vulnerability classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. This affects an unknown part of the file /adms/admin/?page =vehicles/view_trans action. The manipulation of the argument id leads to N/A A-AUT-AUTO- 160323/87	Vendor: aut	omatorwp				
Affected Version(s): * Up to (excluding) 2.5.1Cross-Site Request Forgery (CSRF)28-Feb-20234.3Cross-Site Request Forgery (CSRF) vulnerability in AutomatorWP plugin <= 2.5.0 leads to object delete. CVE ID : CVE-2023- 23992N/AA-AUT-AUTO- 160323/86Vendor: auto_dealer_management_system_projectProduct: auto_dealer_management_system_projectN/AA-AUT-AUTO- 160323/86Affected Version(s): 1.0A vulnerability classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. This affects an unknown part of the file /adms/admin/?page =vehicles/view_trans action. The manipulation of the argument id leads toN/AA-AUT-AUTO- 160323/87						
Cross-Site Request Forgery (CSRF)28-Feb-20234.3Cross-Site Request Forgery (CSRF) vulnerability in AutomatorWP plugin <= 2.5.0 leads to object delete. CVE ID : CVE-2023- 23992N/AA-AUT-AUTO- 160323/86Vendor: auto_dealer_management_system_projectProduct: auto_dealer_management_system_projectAffected Version(s): 1.0Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')A vulnerability classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. This affects an unknown part of the file /adms/admin/?page =vehicles/view_trans action. The manipulation of the argument id leads toN/AA-AUT-AUTO- 160323/87		•	(excluding	o) 2 5 1		
Cross-Site Request Forgery (CSRF)28-Feb-20234.3Forgery (CSRF) vulnerability in AutomatorWP plugin <= 2.5.0 leads to object delete. CVE ID : CVE-2023- 23992N/AA-AUT-AUTO- 160323/86Vendor: auto_dealer_manzement_system_projectCVE ID : CVE-2023- 23992N/AA-AUT-AUTO- 160323/86Vendor: auto_dealer_manzement_system_projectA vulnerability classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. This affects an unknown part of the file /adms/admin/?page =vehicles/view_trans action. The manipulation of the argument id leads toN/AA-AUT-AUTO- 160323/87			(excluding		[
Product: auto_dealer_management_systemAffected Version(s): 1.0Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')A vulnerability classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. This affects an unknown part of the file /adms/admin/?page =vehicles/view_trans action. The manipulation of the argument id leads toN/AA-AUT-AUTO- 160323/87	Cross-Site Request Forgery (CSRF)	28-Feb-2023	4.3	Forgery (CSRF) vulnerability in AutomatorWP plugin <= 2.5.0 leads to object delete. CVE ID : CVE-2023-	N/A	
Product: auto_dealer_management_systemAffected Version(s): 1.0Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')A vulnerability classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. This affects an unknown part of the file /adms/admin/?page =vehicles/view_trans action. The manipulation of the argument id leads toN/AA-AUT-AUTO- 160323/87	Vendor: aut	 co_dealer_mana	agement_	system_project		
Affected Version(s): 1.0Improper Neutralizat ion of Special 			-			
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')18-Feb-20238.8A vulnerability classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. This affects an unknown part of the file /adms/admin/?page =vehicles/view_trans action. The manipulation of the argument id leads toN/AA-AUT-AUTO- 160323/87			ugement			
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')18-Feb-2023aclassified as critical has been found in SourceCodester Auto Dealer Management System 1.0. This affects an unknown part of the file /adms/admin/?page =vehicles/view_trans action. The manipulation of the argument id leads toN/AA-AUT-AUTO- 160323/87	Allected ver	51011(5). 1.0		A 1 1 111		
	Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2023	8.8	classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. This affects an unknown part of the file /adms/admin/?page =vehicles/view_trans action. The manipulation of the	N/A	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10

Page 46 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221481 was assigned to this vulnerability. CVE ID : CVE-2023- 0912		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2023	8.8	A vulnerability classified as critical was found in SourceCodester Auto Dealer Management System 1.0. This vulnerability affects unknown code of the file /adms/admin/?page =vehicles/sell_vehicl e. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-221482 is the identifier assigned to this vulnerability. CVE ID : CVE-2023- 0913	N/A	A-AUT-AUTO- 160323/88
Improper Neutralizat ion of Special Elements used in an	19-Feb-2023	8.8	A vulnerability classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. Affected	N/A	A-AUT-AUTO- 160323/89

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			is an unknown function of the file /adms/admin/?page =user/manage_user. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB- 221490 is the identifier assigned to this vulnerability. CVE ID : CVE-2023- 0915		
N/A	19-Feb-2023	8.8	A vulnerability classified as critical was found in SourceCodester Auto Dealer Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /adms/classes/User s.php. The manipulation leads to improper access controls. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221491. CVE ID : CVE-2023- 0916	N/A	A-AUT-AUTO- 160323/90

0-1

1-2

2-3

3-4 4-5 Page **48** of **859** 5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Vendor: axo	cora								
Product: ax	Product: axcora								
Affected Ver	Affected Version(s): -								
N/A	21-Feb-2023	9.8	An access control issue in Axcora POS #0~gitf77ec09 allows unauthenticated attackers to execute arbitrary commands via unspecified vectors. CVE ID : CVE-2023- 24320	N/A	A-AXC-AXCO- 160323/91				
Vendor: bes	st_pos_manage	ment_sys							
	st_pos_manage								
Affected Ver	sion(s): 1.0								
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	A vulnerability has been found in SourceCodester Best POS Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file billing/index.php?id =9. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The identifier VDB- 221593 was assigned to this vulnerability. CVE ID : CVE-2023- 0946	N/A	A-BES-BEST- 160323/92				

0-1

1-2

2-3

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricte d Upload of File with Dangerous Type	21-Feb-2023	8.8	A vulnerability, which was classified as problematic, has been found in SourceCodester Best POS Management System 1.0. This issue affects some unknown processing of the file index.php?page=site_ settings of the component Image Handler. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-221591. CVE ID : CVE-2023- 0943	N/A	A-BES-BEST- 160323/93
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	A vulnerability, which was classified as problematic, was found in SourceCodester Best POS Management System 1.0. Affected is an unknown function of the file index.php?page=add -category. The manipulation of the argument Name with the input "> leads to cross site scripting. It is</img 	N/A	A-BES-BEST- 160323/94

0-1

1-2

2-3

3-4 4-5 Page **50** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible to launch the attack remotely. The identifier of this vulnerability is VDB- 221592.		
			CVE ID : CVE-2023- 0945		
Vendor: BM	C				
Product: co	ntrol-m				
Affected Ver	sion(s): * Up to	(excluding	g) 9.0.20.214		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL	25-Feb-2023	9.8	A SQL injection vulnerability in BMC Control-M before 9.0.20.214 allows attackers to execute arbitrary SQL commands via the memname JSON field.	N/A	A-BMC-CONT- 160323/95
Injection')			CVE ID : CVE-2023- 26550		
Vendor: boo		L			
	sy_affiliate_lin		-) 2 7 1		
Allected ver	sion(s): * Up to	(excluding			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The Easy Affiliate Links WordPress plugin before 3.7.1 does not validate and escape some of its block options before outputting them back in a page/post where the block is embedded, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	N/A	A-BOO-EASY- 160323/96

0-1

1-2

2-3

5-6

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2023- 0375							
Vendor: bor	Vendor: borg_project									
Product: bo	Product: borg									
Affected Ver	sion(s): * Up to	(excluding	g) 1.1.19							
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Feb-2023	5.3	The Borg theme before 1.1.19 for Backdrop CMS does not sufficiently sanitize path arguments that are passed in via a URL. The function borg_preprocess_pag e in the file template.php does not properly sanitize incoming path arguments before using them. CVE ID : CVE-2023-	https://github .com/backdro p- contrib/borg/ compare/1.x- 1.1.181.x- 1.1.19	A-BOR-BORG- 160323/97					
Vendor: bst	ek		26265							
Product: ur										
	sion(s): 2.1.7									
Allected ver			An XML External							
Improper Restriction of XML External Entity Reference	24-Feb-2023	9.8	An XML External Entity (XXE) vulnerability in urule v2.1.7 allows attackers to execute arbitrary code via uploading a crafted XML file to /urule/common/sav eFile.	N/A	A-BST-URUL- 160323/98					
			CVE ID : CVE-2023- 24189							
Vendor: btc	payserver				<u> </u>					
Product: bt	cpay_server									

0-1

1-2

2-3

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): * Up to	(excluding	g) 1.7.12		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository btcpayserver/btcpay server prior to 1.7.12. CVE ID : CVE-2023- 0879	https://huntr. dev/bounties/ 9464e3c6- 961d-4e23- 8b3d- 07cbb31de54 1, https://github .com/btcpays erver/btcpays erver/commit /f2f3b245c4d 8980d8e54e4 708c796df82 332c3d7	A-BTC-BTCP- 160323/99
Vendor: bus	siness_manage	ment_sys	tem_project	•	
Product: bu	siness_manage	ement_sys	stem		
Affected Ver	sion(s): * Up to	(excluding	g) 2.0.1		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	24-Feb-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository unilogies/bumsys prior to v2.0.1. CVE ID : CVE-2023- 0995	https://huntr. dev/bounties/ 2847b92b- 22c2-4dbc- a9d9- 56a7cd12fe5f, https://github .com/unilogie s/bumsys/co mmit/927214 bd7c475b310 62c56294ff7b 23d523a7219	A-BUS-BUSI- 160323/100
Vendor: can	teen_manager	nent_syst	em_project	I	
Product: ca	nteen_manage	ment_sys	tem		
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements used in an	17-Feb-2023	9.8	Canteen Management System 1.0 is vulnerable to SQL Injection via	N/A	A-CAN-CANT- 160323/101
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10					

Page 53 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			/php_action/getOrde rReport.php. CVE ID : CVE-2023- 23279		
Vendor: cel	linx				I
Product: nv	t_web_server				
Affected Ver	sion(s): 1.0.6.00)2b			
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.5	Cellinx NVT v1.0.6.002b is vulnerable to local file disclosure. CVE ID : CVE-2023- 23063	N/A	A-CEL-NVT 160323/102
Vendor: cer	ebrate-project	:			
Product: ce	rebrate				
Affected Ver	sion(s): 1.12				
N/A	24-Feb-2023	9.1	Cerebrate 1.12 does not properly consider organisation_id during creation of API keys. CVE ID : CVE-2023- 26468	https://github .com/cerebrat e- project/cereb rate/commit/ 7ccf9252470a 23acc38ad6ed 13eecf523e36 8b48	A-CER-CERE- 160323/103
Vendor: cha	mberlain				1
Product: my	yq				
Affected Ver	sion(s): 5.222.0	.32277			
Improper Restriction of Excessive Authentica tion Attempts	21-Feb-2023	9.8	A lack of rate limiting on the password reset endpoint of Chamberlain myQ v5.222.0.32277 (on iOS) allows attackers to compromise user	N/A	A-CHA-MYQ- 160323/104

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accounts via a bruteforce attack.		
			CVE ID : CVE-2023- 24080		
	ingedetection				
	angedetection	<u> </u>			
Affected Ver	sion(s): * Up to	(excluding		Γ	Γ
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	5.4	Changedetection.io before v0.40.1.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the main page. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the URL parameter under the "Add a new change detection watch" function. CVE ID : CVE-2023-	https://github .com/dgtlmoo n/changedete ction.io/issues /1358	A-CHA-CHAN- 160323/105
Vendor: che	eckoutplugins		24769		
	ripe_payments	for woo	commerce		
	sion(s): * Up to				
Cross-Site Request Forgery (CSRF)	28-Feb-2023	4.3	Cross-Site Request Forgery (CSRF) vulnerability in Checkout Plugins Stripe Payments For WooCommerce plugin <= 1.4.10 leads to settings change. CVE ID : CVE-2023- 23865	N/A	A-CHE-STRI- 160323/106

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Vendor: Cis	со	<u> </u>	I	l					
Product: application_policy_infrastructure_controller									
Affected Ver	sion(s): From (i	ncluding)	4.2\\(6\\) Up to (exclu	ding) 5.2\\(7g\\	.)				
Cross-Site Request Forgery (CSRF)	23-Feb-2023	8.8	A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) and Cisco Cloud Network Controller, formerly Cisco Cloud APIC, could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. If the affected user has administrative privileges, these	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-capic- csrfv- DMx6KSwV	A-CIS-APPL- 160323/107				

0-1

1-2

2-3

3-4 4-5 Page **56** of **859** 5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			actions could include modifying the system configuration and creating new privileged accounts.		
			CVE ID : CVE-2023- 20011		
Affected Ver	sion(s): From (i	ncluding)	6.0 Up to (excluding) 6.	0\\(2h\\)	
Cross-Site Request Forgery (CSRF)	23-Feb-2023	8.8	A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) and Cisco Cloud Network Controller, formerly Cisco Cloud APIC, could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-capic- csrfv- DMx6KSwV	A-CIS-APPL- 160323/108

0-1

1-2

2-3

3-4 4-5 Page **57** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			level of the affected user. If the affected user has administrative privileges, these actions could include modifying the system configuration and creating new privileged accounts. CVE ID : CVE-2023- 20011		
Product: clo	oud_network_c	ontroller			
Affected Ver	sion(s): From (i	ncluding)	4.2\\(6\\) Up to (exclu	ding) 25.0\\(5\\)
Cross-Site Request Forgery (CSRF)	23-Feb-2023	8.8	A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) and Cisco Cloud Network Controller, formerly Cisco Cloud APIC, could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-capic- csrfv- DMx6KSwV	A-CIS-CLOU- 160323/109

0-1

1-2

2-3

3-4 4-5 Page **58** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. If the affected user has administrative privileges, these actions could include modifying the system configuration and creating new privileged accounts.		
			CVE ID : CVE-2023- 20011		
Product: no		<u> </u>			
Affected Ver	sion(s): * Up to	(excluding		[
Loop with Unreachabl e Exit Condition ('Infinite Loop')	16-Feb-2023	7.5	node-jose is a JavaScript implementation of the JSON Object Signing and Encryption (JOSE) for web browsers and node.js-based servers. Prior to version 2.2.0, when using the non-default "fallback" crypto back-end, ECC operations in `node- jose` can trigger a Denial-of-Service (DoS) condition, due to a possible infinite loop in an internal calculation. For some ECC operations, this condition is triggered randomly;	https://github .com/cisco/no de- jose/commit/ 901d91508a7 0e3b9bdfc456 88ea07bb4e1 b8210d, https://github .com/cisco/no de- jose/security/ advisories/GH SA-5h4j-qrvg- 9xhw	A-CIS-NODE- 160323/110

0-1

1-2

2-3

3-4 4-5 Page **59** of **859** 5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for others, it can be triggered by malicious input. The issue has been patched in version 2.2.0. Since this issue is only present in the "fallback" crypto implementation, it can be avoided by ensuring that either WebCrypto or the Node `crypto` module is available in the JS environment where `node-jose` is being run. CVE ID : CVE-2023-		
			25653		
	<pre>s_central_softv sion(s): * Up to</pre>		a) 4 2\\(3c\\)		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	A-CIS-UCS 160323/111

0-1

1-2

2-3

3-4 4-5 Page **60** of **859** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Affected Ver	sion(s): From (i	ncluding)	4.0 Up to (excluding) 4.	.0\\(4o\\)	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	A-CIS-UCS 160323/112

0-1

1-2

2-3

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Affected Ver	sion(s): From (i	ncluding)	4.1 Up to (excluding) 4.	1\\(3k\\)	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	A-CIS-UCS 160323/113

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Affected Ver	<mark>sion(s): From (</mark> i	ncluding)	4.2 Up to (excluding) 4.	2\\(2d\\)	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	A-CIS-UCS 160323/114
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 63 of 859	<mark>-6 6-7 7-</mark> 8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Improper Authentica tion	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300- FX3 Series Fabric Extender (FEX)	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc	A-CIS-UCS 160323/115

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. CVE ID : CVE-2023- 20012	o-sa-elyfex- dos-gfvcByx	
Vendor: Cit	rix				
Product: vir	tual_apps_and	_desktop	S		
Affected Ver	sion(s): * Up to	(excluding	g) 2212		
Improper Privilege Manageme nt	16-Feb-2023	7.8	A vulnerability has been identified that, if exploited, could result in a local user elevating their privilege level to NT	https://suppo rt.citrix.com/a rticle/CTX477 616/citrix- virtual-apps- and-desktops-	A-CIT-VIRT- 160323/116

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AUTHORITY\SYSTE M on a Citrix Virtual Apps and Desktops Windows VDA. CVE ID : CVE-2023- 24483	security- bulletin-for- cve20232448 3	
Affected Vers	sion(s): 1912		<u> </u>	I	<u> </u>
Improper Privilege Manageme nt	16-Feb-2023	7.8	A vulnerability has been identified that, if exploited, could result in a local user elevating their privilege level to NT AUTHORITY\SYSTE M on a Citrix Virtual Apps and Desktops Windows VDA. CVE ID : CVE-2023- 24483	https://suppo rt.citrix.com/a rticle/CTX477 616/citrix- virtual-apps- and-desktops- security- bulletin-for- cve20232448 3	A-CIT-VIRT- 160323/117
Affected Vers	sion(s): 2203		1	I	
Improper Privilege Manageme nt	16-Feb-2023	7.8	A vulnerability has been identified that, if exploited, could result in a local user elevating their privilege level to NT AUTHORITY\SYSTE M on a Citrix Virtual Apps and Desktops Windows VDA. CVE ID : CVE-2023- 24483	https://suppo rt.citrix.com/a rticle/CTX477 616/citrix- virtual-apps- and-desktops- security- bulletin-for- cve20232448 3	A-CIT-VIRT- 160323/118
Product: wo	orkspace				<u> </u>
Affected Vers	sion(s): * Up to	(excludin	g) 2212	_	
Incorrect Authorizati on	16-Feb-2023	7.8	Vulnerabilities have been identified that, collectively, allow a standard Windows user to perform operations as SYSTEM on the	https://suppo rt.citrix.com/a rticle/CTX477 617/citrix- workspace- app-for- windows-	A-CIT-WORK- 160323/119
CVSS Scoring S	icale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	³ 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			computer running Citrix Workspace app. CVE ID : CVE-2023- 24485	security- bulletin-for- cve20232448 4- cve20232448 5	
N/A	16-Feb-2023	5.5	A malicious user can cause log files to be written to a directory that they do not have permission to write to. CVE ID : CVE-2023- 24484	https://suppo rt.citrix.com/a rticle/CTX477 617/citrix- workspace- app-for- windows- security- bulletin-for- cve20232448 4- cve20232448 5	A-CIT-WORK- 160323/120
Affected Ver	sion(s): 1912				
Incorrect Authorizati on	16-Feb-2023	7.8	Vulnerabilities have been identified that, collectively, allow a standard Windows user to perform operations as SYSTEM on the computer running Citrix Workspace app. CVE ID : CVE-2023- 24485	https://suppo rt.citrix.com/a rticle/CTX477 617/citrix- workspace- app-for- windows- security- bulletin-for- cve20232448 4- cve20232448 5	A-CIT-WORK- 160323/121
N/A	16-Feb-2023	5.5	A malicious user can cause log files to be written to a directory that they do not have permission to write to. CVE ID : CVE-2023- 24484	https://suppo rt.citrix.com/a rticle/CTX477 617/citrix- workspace- app-for- windows- security- bulletin-for- cve20232448	A-CIT-WORK- 160323/122

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				4- cve20232448 5	
Affected Ver	sion(s): 2203.1				
Incorrect Authorizati on	16-Feb-2023	7.8	Vulnerabilities have been identified that, collectively, allow a standard Windows user to perform operations as SYSTEM on the computer running Citrix Workspace app. CVE ID : CVE-2023- 24485	https://suppo rt.citrix.com/a rticle/CTX477 617/citrix- workspace- app-for- windows- security- bulletin-for- cve20232448 4- cve20232448 5	A-CIT-WORK- 160323/123
N/A	16-Feb-2023	5.5	A malicious user can cause log files to be written to a directory that they do not have permission to write to. CVE ID : CVE-2023- 24484	https://suppo rt.citrix.com/a rticle/CTX477 617/citrix- workspace- app-for- windows- security- bulletin-for- cve20232448 4- cve20232448 5	A-CIT-WORK- 160323/124
Vendor: cla	sh_project				
Product: cla	ish				
Affected Ver	sion(s): 0.20.12				
Incorrect Permission Assignmen t for Critical Resource	23-Feb-2023	9.8	Clash for Windows v0.20.12 was discovered to contain a remote code execution (RCE) vulnerability which is exploited via overwriting the	N/A	A-CLA-CLAS- 160323/125

 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
			configuration file (cfw-setting.yaml).		
			CVE ID : CVE-2023- 24205		
Vendor: clas	ss_and_exam_t	imetablir	ng_system_project		
	iss_and_exam_t	timetabli	ng_system		
Affected Vers	sion(s): 1.0				-
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	26-Feb-2023	8.8	A vulnerability classified as critical was found in SourceCodester Class and Exam Timetabling System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/index3.php of the component POST Parameter Handler. The manipulation of the argument password leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221797 was assigned to this vulnerability. CVE ID : CVE-2023- 1039	N/A	A-CLA-CLAS- 160323/126
	nics_patient_m				
Affected Vers					

0-1

1-2

2-3

3-4 4-5 Page **69** of **859** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	8.8	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been classified as critical. Affected is an unknown function of the file update_user.php. The manipulation of the argument user_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB- 221784. CVE ID : CVE-2023- 1035	N/A	A-CLI-CLIN- 160323/127
Vendor: cor					
	rreos_oficial sion(s): * Up to	(including	ı) 1 2 0 2		
		Cinciuuiii	The Correos Oficial		
Files or Directories Accessible to External Parties	27-Feb-2023	7.5	WordPress plugin through 1.2.0.2 does not have an authorization check user input validation when generating a file path, allowing unauthenticated attackers to download arbitrary files from the server. CVE ID : CVE-2023- 0331	N/A	A-COR-CORR- 160323/128

0-1

1-2

2-3

3-4 4-5 Page **70** of **859** 6-7

5-6

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Vendor: cov	resa	I		L		
Product: dlt-daemon						
Affected Ver	sion(s): * Up to	(including	g) 2.18.8			
Missing Release of Memory after Effective Lifetime	27-Feb-2023	7.5	An issue was discovered in the Connected Vehicle Systems Alliance (COVESA; formerly GENIVI) dlt-daemon through 2.18.8. Dynamic memory is not released after it is allocated in dlt- control-common.c.	https://github .com/COVESA /dlt- daemon/pull/ 441/commits /b6149e203f9 19c899fefc70 2a17fbb78bde c3700	A-COV-DLT 160323/129	
			CVE ID : CVE-2023- 26257			
Vendor: Cra	ftercms					
Product: cra	after_cms					
Affected Ver	sion(s): From (i	ncluding)	3.1.0 Up to (including)	3.1.26		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Crafter Studio on Linux, MacOS, Windows, x86, ARM, 64 bit allows SQL Injection.This issue affects CrafterCMS v4.0 from 4.0.0 through 4.0.1, and v3.1 from 3.1.0 through 3.1.26.	https://docs.c raftercms.org /en/4.0/secur ity/advisory.h tml#cv- 2023021701	A-CRA-CRAF- 160323/130	
			CVE ID : CVE-2023- 26020			
Affected Ver	sion(s): From (i	ncluding)	4.0.0 Up to (including)	4.0.1		

0-1

1-2

2-3

3-4 4-5 Page **71** of **859** 5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Crafter Studio on Linux, MacOS, Windows, x86, ARM, 64 bit allows SQL Injection.This issue affects CrafterCMS v4.0 from 4.0.0 through 4.0.1, and v3.1 from 3.1.0 through 3.1.26. CVE ID : CVE-2023- 26020	https://docs.c raftercms.org /en/4.0/secur ity/advisory.h tml#cv- 2023021701	A-CRA-CRAF- 160323/131
Vendor: cra	sm_project				
Product: cra	asm				
Affected Ver	sion(s): 1.8-3				
NULL Pointer Dereferenc e	27-Feb-2023	7.5	In crasm 1.8-3, invalid input validation, specific files passed to the command line application, can lead to a NULL pointer dereference in the function Xasc.	https://github .com/colinbou rassa/crasm/ pull/7	A-CRA-CRAS- 160323/132
			CVE ID : CVE-2023- 23108		
Divide By Zero	27-Feb-2023	7.5	In crasm 1.8-3, invalid input validation, specific files passed to the command line application, can lead to a divide by zero	https://github .com/colinbou rassa/crasm/ pull/7	A-CRA-CRAS- 160323/133

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fault in the function opdiv. CVE ID : CVE-2023- 23109		
Vendor: dat	aease			I	I
Product: da	taease				
Affected Ver	sion(s): * Up to	(excluding	g) 1.18.3		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	28-Feb-2023	5.4	DataEase is an open source data visualization and analysis tool. When saving a dashboard on the DataEase platform saved data can be modified and store malicious code. This vulnerability can lead to the execution of malicious code stored by the attacker on the server side when the user accesses the dashboard. The vulnerability has been fixed in version 1.18.3. CVE ID : CVE-2023- 25807	https://github .com/dataease /dataease/co mmit/cc94fb8 e69ddbb37c9 6d02ec0f0ddc d74273ef49, https://github .com/dataease /dataease/sec urity/advisori es/GHSA- xj3h-3wmw- j5vf	A-DAT-DATA- 160323/134
	vinci_project				
Product: da					
	sion(s): 0.3.0				
Improper Neutralizat ion of Special Elements used in an SQL Command	27-Feb-2023	9.8	Davinci v0.3.0-rc was discovered to contain a SQL injection vulnerability via the copyDisplay function.	N/A	A-DAV-DAVI- 160323/135
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 73 of 859	-6 6-7 7-8	8 8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			CVE ID : CVE-2023- 24206		
Vendor: Del	1				
Product: mu	ultifunction_pr	inter_e52	25w_driver_and_softwa	are_suite	
Affected Ver	sion(s): * Up to	(excluding	g) 1.047.2022_a05		
N/A	21-Feb-2023	7.8	Dell Multifunction Printer E525w Driver and Software Suite, versions prior to 1.047.2022, A05, contain a local privilege escalation vulnerability that could be exploited by malicious users to compromise the affected system	https://www. dell.com/supp ort/kbdoc/en- us/00020839 6/dsa-2023- 043	A-DEL-MULT- 160323/136
Product: see	cure_connect_g	vateway	CVE ID : CVE-2023- 24575		
	sion(s): 5.12.00	•			
Use of a Broken or Risky Cryptograp hic Algorithm	17-Feb-2023	5.9	Dell Secure Connect Gateway (SCG) version 5.14.00.12 contains a broken cryptographic algorithm vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by performing MitM attacks and let attackers obtain sensitive information. CVE ID : CVE-2023- 23695	https://www. dell.com/supp ort/kbdoc/en- us/00020846 2/dsa-2023- 020-dell- secure- connect- gateway- security- update-for- multiple- vulnerabilities	A-DEL-SECU- 160323/137

0-1

1-2

2-3

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): 5.14.00	.12			
Use of a Broken or Risky Cryptograp hic Algorithm	17-Feb-2023	5.9	Dell Secure Connect Gateway (SCG) version 5.14.00.12 contains a broken cryptographic algorithm vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by performing MitM attacks and let attackers obtain sensitive information. CVE ID : CVE-2023- 23695	https://www. dell.com/supp ort/kbdoc/en- us/00020846 2/dsa-2023- 020-dell- secure- connect- gateway- security- update-for- multiple- vulnerabilities	A-DEL-SECU- 160323/138
Vendor: del	taww			I	
Product: dia	energie				
Affected Vers	sion(s): * Up to	(excluding	g) 1.9.03.001		
Files or Directories Accessible to External Parties	17-Feb-2023	8.8	The affected product DIAEnergie (versions prior to v1.9.03.001) contains improper authorization, which could allow an unauthorized user to bypass authorization and access privileged functionality. CVE ID : CVE-2023- 0822	N/A	A-DEL-DIAE- 160323/139
Vendor: deno					
Product: deno					
Affected Version(s): * Up to (excluding) 1.31.0					
N/A	25-Feb-2023	7.5	Versions of the package deno before	https://github .com/denolan	A-DEN-DENO- 160323/140
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 75 of 859	<mark>-6 6-7 7-</mark> 8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vordor de			1.31.0 are vulnerable to Regular Expression Denial of Service (ReDoS) due to the upgradeWebSocket function, which contains regexes in the form of /s*,s*/, used for splitting the Connection/Upgrade header. A specially crafted Connection/Upgrade header can be used to significantly slow down a web socket server. CVE ID : CVE-2023- 26103	d/deno/pull/ 17722, https://github .com/denolan d/deno/com mit/cf06a7c7 e672880e1b3 8598fe445e2c 50b4a9d06	
			_reservation_system_p	project	
Affected Ver		ointmen	t_reservation_system		
Allected ver			A vulnerability was		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	26-Feb-2023	9.8	found in SourceCodester Dental Clinic Appointment Reservation System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /APR/login.php of the component POST Parameter Handler. The manipulation of the argument username leads to sql injection. The attack may be	N/A	A-DEN-DENT- 160323/141

0-1

1-2

2-3

3-4 4-5 Page **76** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB- 221795.		
			CVE ID : CVE-2023- 1037		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	26-Feb-2023	6.1	A vulnerability was found in SourceCodester Dental Clinic Appointment Reservation System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /APR/signup.php of the component POST Parameter Handler. The manipulation of the argument firstname leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB- 221794 is the identifier assigned to this vulnerability. CVE ID : CVE-2023- 1036	N/A	A-DEN-DENT- 160323/142
Vendor: dev	vowl				
	al_media_libra sion(s): * Up to	-	g) 4.18.29		
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	<u>8-9</u> 9-10
			Page 77 of 859	· · ·	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The Real Media Library WordPress plugin before 4.18.29 does not sanitise and escape the created folder names, which could allow users with the role of author and above to perform Stored Cross-Site Scripting attacks. CVE ID : CVE-2023-	N/A	A-DEV-REAL- 160323/143
			0285		
Vendor: doc	cmosis				I
Product: tor	rnado				
Affected Vers	sion(s): * Up to	(excluding	g) 2.9.5		
N/A	28-Feb-2023	8.8	An issue was discovered in Docmosis Tornado prior to version 2.9.5. An authenticated attacker can change the Office directory setting pointing to an arbitrary remote network path. This triggers the execution of the soffice binary under the attackers control leading to arbitrary remote code execution (RCE). CVE ID : CVE-2023- 25266	N/A	A-DOC-TORN- 160323/144
Improper Authentica tion	28-Feb-2023	7.5	An issue was discovered in Docmosis Tornado prior to version 2.9.5. An	N/A	A-DOC-TORN- 160323/145
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 78 of 859	-6 6-7 7-8	8 8-9 9-10

Page **78** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker can bypass the authentication check filter completely by introducing a specially crafted request with relative path segments. CVE ID : CVE-2023- 25264		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Feb-2023	7.5	Docmosis Tornado <= 2.9.4 is vulnerable to Directory Traversal leading to the disclosure of arbitrary content on the file system. CVE ID : CVE-2023- 25265	N/A	A-DOC-TORN- 160323/146
Vendor: doc	tors_appointn	nent_syst	em_project		
Product: do	ctors_appointr	nent_syst	em		
Affected Vers	sion(s): 1.0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	A vulnerability was found in SourceCodester Doctors Appointment System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /edoc/doctor/patien t.php. The manipulation of the argument search12 leads to sql injection. The attack can be launched remotely.	N/A	A-DOC-DOCT- 160323/147
CVSS Scoring S	cale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10

Page **79** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. The identifier VDB-221821 was assigned to this vulnerability.		
			CVE ID : CVE-2023- 1056		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	A vulnerability was found in SourceCodester Doctors Appointment System 1.0. It has been rated as critical. Affected by this issue is the function edoc of the file login.php. The manipulation of the argument usermail leads to sql injection. VDB-221822 is the identifier assigned to this vulnerability. CVE ID : CVE-2023- 1057	N/A	A-DOC-DOCT- 160323/148
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	A vulnerability classified as critical has been found in SourceCodester Doctors Appointment System 1.0. This affects an unknown part of the file create- account.php. The manipulation of the argument newemail leads to sql injection. It is possible to initiate the attack remotely. The exploit	N/A	A-DOC-DOCT- 160323/149

0-1

1-2

2-3

3-4 4-5 Page 80 of 859

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221823.		
			CVE ID : CVE-2023- 1058		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	A vulnerability classified as critical was found in SourceCodester Doctors Appointment System 1.0. This vulnerability affects unknown code of the file /admin/doctors.php of the component Parameter Handler. The manipulation of the argument search leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221824. CVE ID : CVE-2023- 1059	N/A	A-DOC-DOCT- 160323/150
Improper Neutralizat ion of Special Elements used in an SQL Command	27-Feb-2023	8.8	A vulnerability, which was classified as critical, has been found in SourceCodester Doctors Appointment System 1.0. This issue affects some unknown	N/A	A-DOC-DOCT- 160323/151

0-1

1-2

2-3

7-8

8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			processing of the file /admin/edit- doc.php. The manipulation of the argument oldmail leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221825 was assigned to this vulnerability. CVE ID : CVE-2023- 1061		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	A vulnerability, which was classified as critical, was found in SourceCodester Doctors Appointment System 1.0. Affected is an unknown function of the file /admin/add- new.php of the component Parameter Handler. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB- 221826 is the identifier assigned to this vulnerability. CVE ID : CVE-2023- 1062	N/A	A-DOC-DOCT- 160323/152

0-1

1-2

2-3

3-4 4-5 Page **82** of **859** 5-6

7-8

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	A vulnerability has been found in SourceCodester Doctors Appointment System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/patient.php of the component Parameter Handler. The manipulation of the argument search leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB- 221827. CVE ID : CVE-2023- 1063	N/A	A-DOC-DOCT- 160323/153
Vendor: dol	phinphp_proje	ect			
Product: do	lphinphp				
Affected Ver	sion(s): * Up to	(including	g) 1.5.1		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	21-Feb-2023	9.8	A vulnerability was found in DolphinPHP up to 1.5.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file common.php of the component Incomplete Fix CVE-	N/A	A-DOL-DOLP- 160323/154

0-1

1-2

2-3

6-7 7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2021-46097. The manipulation of the argument id leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221551.		
			CVE ID : CVE-2023- 0935		
Vendor: dor					
Product: iko					
	sion(s): * Up to	(excluding	g) 2.8.6	ſ	Ι
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	9.8	Domotica Labs srl Ikon Server before v2.8.6 was discovered to contain a SQL injection vulnerability. CVE ID : CVE-2023- 24253	N/A	A-DOM-IKON- 160323/155
Vendor: dor	nation_block_f	or_paypal	_project		
Product: do	nation_block_f	or_paypa	1		
Affected Ver	sion(s): * Up to	(excluding	g) 2.1.0		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	The Donation Block For PayPal WordPress plugin before 2.1.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode	N/A	A-DON-DONA- 160323/156

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. CVE ID : CVE-2023- 0535		
Vendor: ecis	sp				
Product: esp	pcms				
Affected Vers	sion(s): p8.2112	20101			
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	7.2	An issue was discovered in ESPCMS P8.21120101 after logging in to the background, there is a SQL injection vulnerability in the function node where members are added. CVE ID : CVE-2023- 23007	N/A	A-ECI-ESPC- 160323/157
Vendor: em	bedsocial				
Product: em	bedsocial				
Affected Vers	sion(s): * Up to	(excluding		T	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The EmbedSocial WordPress plugin before 1.1.28 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform	N/A	A-EMB-EMBE- 160323/158
CVSS Scoring S	icale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-	8 8-9 9-10
			Page 85 of 859		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Stored Cross-Site Scripting attacks CVE ID : CVE-2023- 0371		
Product: em	ibedstories				
Affected Ver	sion(s): * Up to	(excluding	g) 0.7.5		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The EmbedStories WordPress plugin before 0.7.5 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	N/A	A-EMB-EMBE- 160323/159
			CVE ID : CVE-2023- 0372		
		<u> </u>	nt_system_project		
	ployee_task_n	nanagem	ent_system		
Affected Ver	sion(s): 1.0			Γ	Γ
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2023	8.8	A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file edit- task.php. The manipulation of the argument task_id leads to sql injection.	N/A	A-EMP-EMPL- 160323/160

0-1

1-2

2-3

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221452. CVE ID : CVE-2023-		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2023	8.8	0903 A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file task- details.php. The manipulation of the argument task_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221453 was assigned to this vulnerability. CVE ID : CVE-2023- 0904	N/A	A-EMP-EMPL- 160323/161
Improper Authentica tion	18-Feb-2023	7.5	A vulnerability classified as critical has been found in SourceCodester Employee Task Management System 1.0. Affected is an unknown function of	N/A	A-EMP-EMPL- 160323/162

0-1

1-2

2-3

5-6

6-7

			the file changePasswordFor Employee.php. The manipulation leads to improper authentication. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-221454 is the identifier assigned to this		
			vulnerability. CVE ID : CVE-2023- 0905		
Vendor: eterna	al_terminal_j	project	0703		
Product: eterna	al_terminal				
Affected Version	n(s): 6.2.1				
Improper Link Resolution Before File 16 Access ('Link Following')	6-Feb-2023	6.3	In Eternal Terminal 6.2.1, TelemetryService uses fixed paths in /tmp. For example, a local attacker can create /tmp/.sentry- native-etserver with mode 0777 before the etserver process is started. The attacker can choose to read sensitive information from that file, or modify the information in that file. CVE ID : CVE-2023- 23558	http://www.o penwall.com/l ists/oss- security/2023 /02/16/1	A-ETE-ETER- 160323/163
Vendor: execut	tablebooks				
Product: marke					

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.2.0					
N/A	22-Feb-2023	5.5	Denial of service could be caused to the command line interface of markdown-it-py, before v2.2.0, if an attacker was allowed to use invalid UTF-8 characters as input. CVE ID : CVE-2023- 26302	https://github .com/executa blebooks/mar kdown-it- py/commit/5 3ca3e9c2b9e9 b295f6abf7f4 ad2730a9b70f 68c	A-EXE-MARK- 160323/164
N/A	23-Feb-2023	5.5	Denial of service could be caused to markdown-it-py, before v2.2.0, if an attacker was allowed to force null assertions with specially crafted input. CVE ID : CVE-2023- 26303	https://github .com/executa blebooks/mar kdown-it- py/commit/a e03c6107dfa1 8e648f6fdd12 80f5b89092d 5d49	A-EXE-MARK- 160323/165
Vendor: Filseclab					
Product: twister_antivirus					
Affected Version(s): 8.17					
Improper Access Control	24-Feb-2023	7.8	A vulnerability was found in Twister Antivirus 8.17. It has been declared as critical. This vulnerability affects unknown code in the library filmfd.sys of the component IoControlCode Handler. The manipulation leads to improper access controls. The attack needs to be	https://github .com/zeze- zeze/Window sKernelVuln/t ree/master/C VE-2023- 1007	A-FIL-TWIS- 160323/166

0-1

1-2

2-3

3-4 4-5 Page **89** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221740.		
			CVE ID : CVE-2023- 1007		
Improper Resource Shutdown or Release	18-Feb-2023	5.5	A vulnerability, which was classified as problematic, has been found in Filseclab Twister Antivirus 8.17. Affected by this issue is some unknown functionality in the library ffsmon.sys of the component loControlCode Handler. The manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221456. CVE ID : CVE-2023- 0907	N/A	A-FIL-TWIS- 160323/167
Improper Resource Shutdown or Release	24-Feb-2023	5.5	A vulnerability was found in Twister Antivirus 8.17. It has been rated as problematic. This issue affects some unknown processing in the library filmfd.sys of the	https://github .com/zeze- zeze/Window sKernelVuln/t ree/master/C VE-2023- 1008	A-FIL-TWIS- 160323/168

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component IoControlCode Handler. The manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier VDB-221741 was assigned to this vulnerability. CVE ID : CVE-2023- 1008		
Vendor: Flat	tpress				
Product: fla	tpress				
Affected Vers	sion(s): * Up to	(including	g) 1.2.1		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	9.8	Path Traversal in GitHub repository flatpressblog/flatpre ss prior to 1.3. CVE ID : CVE-2023- 0947	https://huntr. dev/bounties/ 7379d702- 72ff-4a5d- bc68- 00729001549 6, https://github .com/flatpress blog/flatpress /commit/9c4 e5d6567e446 c472f3adae3b 2fe612f66871 c7	A-FLA-FLAT- 160323/169
Vendor: For	-				
•	a_policy_agen				
Affected Vers	sion(s): * Up to	(including	g) 5.10.1		
Improper Limitation of a Pathname	28-Feb-2023	9.8	Relative Path Traversal vulnerability in ForgeRock Access	https://backst age.forgerock. com/knowled	A-FOR-JAVA- 160323/170
			0		
CVSS Scoring S	cale 0-1	1-2 2		-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Management Java Policy Agent allows Authentication Bypass. This issue affects Access Management Java Policy Agent: all versions up to 5.10.1 CVE ID : CVE-2023- 0511	ge/kb/article/ a21576868	
	eb_policy_agen			1	
Affected Ver	sion(s): * Up to	(including	g) 5.10.1		-
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Feb-2023	9.8	Relative Path Traversal vulnerability in ForgeRock Access Management Web Policy Agent allows Authentication Bypass. This issue affects Access Management Web Policy Agent: all versions up to 5.10.1 CVE ID : CVE-2023- 0339	https://backst age.forgerock. com/knowled ge/kb/article/ a21576868	A-FOR-WEB 160323/171
Vendor: For	tinet				
Product: for	rtinac				
Affected Ver	sion(s): 8.3.7				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation vulnerability [CWE- 79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and below, 8.6.5 and below, 8.5.4 and	https://fortig uard.com/psir t/FG-IR-22- 260	A-FOR-FORT- 160323/172

0-1

1-2

2-3

3-4 4-5 Page **92** of **859** 5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. CVE ID : CVE-2023-		
Affected Ver	sion(s): 9.4.0		22638		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation vulnerability [CWE- 79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 9.1.8 and below, 8.8.11 and below, 8.8.11 and below, 8.6.5 and below, 8.6.5 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. CVE ID : CVE-2023- 22638	https://fortig uard.com/psir t/FG-IR-22- 260	A-FOR-FORT- 160323/173
Affected Ver	sion(s): 9.4.1				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation vulnerability [CWE- 79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and	https://fortig uard.com/psir t/FG-IR-22- 260	A-FOR-FORT- 160323/174

0-1

1-2

2-3

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below, 8.6.5 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. CVE ID : CVE-2023-		
			22638		
Affected Ver	sion(s): From (i	ncluding)	8.5.0 Up to (including)	8.5.4	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation vulnerability [CWE- 79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and below, 8.6.5 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. CVE ID : CVE-2023- 22638	https://fortig uard.com/psir t/FG-IR-22- 260	A-FOR-FORT- 160323/175
Affected Ver	sion(s): From (i	ncluding)	8.6.0 Up to (including)	8.6.5	
Improper Neutralizat ion of Input During Web Page Generation	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation vulnerability [CWE- 79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and	https://fortig uard.com/psir t/FG-IR-22- 260	A-FOR-FORT- 160323/176

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			below, 8.8.11 and below, 8.7.6 and below, 8.6.5 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. CVE ID : CVE-2023- 22638		
Affected Ver	<mark>sion(s): From (</mark> i	ncluding)	8.7.0 Up to (including)	8.7.6	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation vulnerability [CWE- 79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 9.1.8 and below, 8.8.11 and below, 8.8.11 and below, 8.6.5 and below, 8.6.5 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. CVE ID : CVE-2023- 22638	https://fortig uard.com/psir t/FG-IR-22- 260	A-FOR-FORT- 160323/177
Affected Ver	sion(s): From (i	ncluding)	8.8.0 Up to (including)	8.8.11	
Improper Neutralizat ion of Input During Web Page	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation vulnerability [CWE- 79] in FortiNAC 9.4.1	https://fortig uard.com/psir t/FG-IR-22- 260	A-FOR-FORT- 160323/178

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			and below, 9.2.6 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and below, 8.6.5 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. CVE ID : CVE-2023-		
Affected Vor	rion(c): From (i	ncluding	22638 9.1.0 Up to (including)	010	
			Several improper		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	16-Feb-2023	5.4	neutralization of inputs during web page generation vulnerability [CWE- 79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and below, 8.7.6 and below, 8.5.4 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. CVE ID : CVE-2023-	https://fortig uard.com/psir t/FG-IR-22- 260	A-FOR-FORT- 160323/179
Affected Vers	sion(s): From (i	ncluding)	22638 9.2.0 Up to (including)	9.2.7	
Improper Neutralizat ion of Input	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation	https://fortig uard.com/psir t/FG-IR-22- 260	A-FOR-FORT- 160323/180
CVSS Scoring S	cale 0-1	1-2 2	-3 3-4 4-5 5	<mark>-6 6-7 7-</mark> 8	<u>8 8-9 9-10</u>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			vulnerability [CWE- 79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and below, 8.6.5 and below, 8.6.5 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. CVE ID : CVE-2023- 22638		
Product: for	rtiweb				
Affected Ver	sion(s): 6.4.0				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	Multiple improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below may allow an authenticated attacker to execute unauthorized code or commands via crafted parameters of HTTP requests. CVE ID : CVE-2023- 23779	N/A	A-FOR-FORT- 160323/181
Improper Limitation	16-Feb-2023	6.5	A relative path traversal	https://fortig uard.com/psir	A-FOR-FORT- 160323/182

0-1

1-2

2-3

3-4 4-5 Page **97** of **859**

5 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			vulnerability [CWE- 23] in FortiWeb version 7.0.1 and below, 6.4 all versions, 6.3 all versions, 6.2 all versions may allow an authenticated user to obtain unauthorized access to files and data via specifically crafted web requests.	t/FG-IR-22- 142	
			CVE ID : CVE-2023- 23778		
Affected Ver	sion(s): 6.4.1				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	Multiple improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below may allow an authenticated attacker to execute unauthorized code or commands via crafted parameters of HTTP requests. CVE ID : CVE-2023- 23779	N/A	A-FOR-FORT- 160323/183
Improper Limitation of a Pathname to a	16-Feb-2023	6.5	A relative path traversal vulnerability [CWE- 23] in FortiWeb version 7.0.1 and	https://fortig uard.com/psir t/FG-IR-22- 142	A-FOR-FORT- 160323/184

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			below, 6.4 all versions, 6.3 all versions, 6.2 all versions may allow an authenticated user to obtain unauthorized access to files and data via specifically crafted web requests. CVE ID : CVE-2023- 23778		
Affected Ver	sion(s): 6.4.2				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	Multiple improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below may allow an authenticated attacker to execute unauthorized code or commands via crafted parameters of HTTP requests. CVE ID : CVE-2023- 23779	N/A	A-FOR-FORT- 160323/185
Improper Limitation of a Pathname to a Restricted Directory	16-Feb-2023	6.5	A relative path traversal vulnerability [CWE- 23] in FortiWeb version 7.0.1 and below, 6.4 all versions, 6.3 all versions, 6.2 all	https://fortig uard.com/psir t/FG-IR-22- 142	A-FOR-FORT- 160323/186

0-1

1-2

2-3

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			versions may allow an authenticated user to obtain unauthorized access to files and data via specifically crafted web requests. CVE ID : CVE-2023-		
			23778		
Affected Ver	sion(s): 7.0.0				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	Multiple improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below may allow an authenticated attacker to execute unauthorized code or commands via crafted parameters of HTTP requests. CVE ID : CVE-2023- 23779	N/A	A-FOR-FORT- 160323/187
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	6.5	A relative path traversal vulnerability [CWE- 23] in FortiWeb version 7.0.1 and below, 6.4 all versions, 6.3 all versions, 6.2 all versions may allow an authenticated user to obtain	https://fortig uard.com/psir t/FG-IR-22- 142	A-FOR-FORT- 160323/188

0-1

1-2

2-3

3-4 4-5 Page **100** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to files and data via specifically crafted web requests.		
			CVE ID : CVE-2023- 23778		
Affected Ver	sion(s): 7.0.1			<u> </u>	I
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	Multiple improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below may allow an authenticated attacker to execute unauthorized code or commands via crafted parameters of HTTP requests. CVE ID : CVE-2023- 23779	N/A	A-FOR-FORT- 160323/189
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	6.5	A relative path traversal vulnerability [CWE- 23] in FortiWeb version 7.0.1 and below, 6.4 all versions, 6.3 all versions, 6.2 all versions may allow an authenticated user to obtain unauthorized access to files and data via	https://fortig uard.com/psir t/FG-IR-22- 142	A-FOR-FORT- 160323/190

0-1

1-2

2-3

3-4 4-5 Page **101** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specifically crafted web requests. CVE ID : CVE-2023- 23778		
Affected Ver	sion(s): From (i	ncluding)	5.6.0 Up to (excluding)	5.9.2	
Out-of- bounds Write	16-Feb-2023	7.8	A stack-based buffer overflow in Fortinet FortiWeb 6.4 all versions, FortiWeb versions 6.3.17 and earlier, FortiWeb versions 6.2.6 and earlier, FortiWeb versions 6.1.2 and earlier, FortiWeb versions 6.0.7 and earlier, FortiWeb versions 5.9.1 and earlier, FortiWeb 5.8 all versions, FortiWeb 5.7 all versions, FortiWeb 5.6 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments. CVE ID : CVE-2023- 25602	https://fortig uard.com/psir t/FG-IR-21- 234	A-FOR-FORT- 160323/191
Affected Ver	sion(s): From (i	ncluding)	6.0.0 Up to (excluding)	6.0.8	
Out-of- bounds Write	16-Feb-2023	7.8	A stack-based buffer overflow in Fortinet FortiWeb 6.4 all versions, FortiWeb versions 6.3.17 and earlier, FortiWeb versions 6.2.6 and earlier, FortiWeb versions 6.1.2 and	https://fortig uard.com/psir t/FG-IR-21- 234	A-FOR-FORT- 160323/192

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			earlier, FortiWeb versions 6.0.7 and earlier, FortiWeb versions 5.9.1 and earlier, FortiWeb 5.8 all versions, FortiWeb 5.7 all versions, FortiWeb 5.6 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments. CVE ID : CVE-2023- 25602			
Affected Vers	<mark>sion(s): From (i</mark>	ncluding)	6.0.0 Up to (including)	6.2.7		
Out-of- bounds Write	16-Feb-2023	7.8	A heap-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, FortiWeb version 6.3.0 through 6.3.19, FortiWeb 6.4 all versions, FortiWeb 6.2 all versions, FortiWeb 6.1 all versions allows attacker to escalation of privilege via specifically crafted arguments to existing commands. CVE ID : CVE-2023- 23782	https://fortig uard.com/psir t/FG-IR-22- 111	A-FOR-FORT- 160323/193	
	sion(s): From (i	ncluding)	6.1.0 Up to (excluding) A stack-based buffer	6.1.3 https://fortig		
Out-of- bounds Write	16-Feb-2023	7.8	overflow in Fortinet FortiWeb 6.4 all versions, FortiWeb	uard.com/psir t/FG-IR-21- 234	A-FOR-FORT- 160323/194	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 103 of 859						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 6.3.17 and earlier, FortiWeb versions 6.2.6 and earlier, FortiWeb versions 6.1.2 and earlier, FortiWeb versions 6.0.7 and earlier, FortiWeb versions 5.9.1 and earlier, FortiWeb 5.8 all versions, FortiWeb 5.7 all versions, FortiWeb 5.6 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments. CVE ID : CVE-2023- 25602		
Affected Ver	<mark>sion(s): From (</mark> i	ncluding)	6.2.0 Up to (excluding) A stack-based buffer	6.2.7	
Out-of- bounds Write	16-Feb-2023	7.8	overflow in Fortinet FortiWeb 6.4 all versions, FortiWeb versions 6.3.17 and earlier, FortiWeb versions 6.2.6 and earlier, FortiWeb versions 6.1.2 and earlier, FortiWeb versions 6.0.7 and earlier, FortiWeb versions 5.9.1 and earlier, FortiWeb 5.8 all versions, FortiWeb 5.7 all versions, FortiWeb 5.6 all versions allows attacker to	https://fortig uard.com/psir t/FG-IR-21- 234	A-FOR-FORT- 160323/195

0-1

1-2

2-33-44-5Page 104 of 859

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute unauthorized code or commands via specially crafted command arguments.		
			CVE ID : CVE-2023- 25602		
Affected Ver	sion(s): From (i	ncluding)	6.2.3 Up to (including)	6.2.7	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	6.5	A relative path traversal vulnerability [CWE- 23] in FortiWeb version 7.0.1 and below, 6.4 all versions, 6.3 all versions, 6.2 all versions may allow an authenticated user to obtain unauthorized access to files and data via specifically crafted web requests. CVE ID : CVE-2023- 23778	https://fortig uard.com/psir t/FG-IR-22- 142	A-FOR-FORT- 160323/196
Affected Ver	sion(s): From (i	ncluding)	6.3.0 Up to (excluding)	6.3.18	I
Out-of- bounds Write	16-Feb-2023	7.8	A stack-based buffer overflow in Fortinet FortiWeb 6.4 all versions, FortiWeb versions 6.3.17 and earlier, FortiWeb versions 6.2.6 and earlier, FortiWeb versions 6.1.2 and earlier, FortiWeb versions 6.0.7 and earlier, FortiWeb versions 5.9.1 and earlier, FortiWeb 5.8 all versions,	https://fortig uard.com/psir t/FG-IR-21- 234	A-FOR-FORT- 160323/197

0-1

1-2

2-33-44-5Page 105 of 859

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiWeb 5.7 all versions, FortiWeb 5.6 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments. CVE ID : CVE-2023- 25602	(2 20	
Affected Ver	sion(s): From (i	ncluding)	6.3.0 Up to (excluding)	6.3.20	
Out-of- bounds Write	16-Feb-2023	8.8	A stack-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, Fortinet FortiWeb version 6.3.6 through 6.3.19, Fortinet FortiWeb 6.4 all versions allows attacker to escalation of privilege via specifically crafted HTTP requests. CVE ID : CVE-2023- 23780	https://fortig uard.com/psir t/FG-IR-22- 118	A-FOR-FORT- 160323/198
Out-of- bounds Write	16-Feb-2023	8.8	A stack-based buffer overflow vulnerability [CWE- 121] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below SAML server configuration may allow an authenticated attacker to achieve	https://fortig uard.com/psir t/FG-IR-22- 151	A-FOR-FORT- 160323/199

0-1

1-2

2-33-44-5Page 106 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution via specifically crafted XML files.		
			CVE ID : CVE-2023- 23781		
Out-of- bounds Write	16-Feb-2023	7.8	A heap-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, FortiWeb version 6.3.0 through 6.3.19, FortiWeb 6.4 all versions, FortiWeb 6.2 all versions, FortiWeb 6.1 all versions allows attacker to escalation of privilege via specifically crafted arguments to existing commands. CVE ID : CVE-2023- 23782	https://fortig uard.com/psir t/FG-IR-22- 111	A-FOR-FORT- 160323/200
Affected Ver	sion(s): From (i	ncluding)	6.3.0 Up to (including)	6.3.21	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	6.5	A relative path traversal vulnerability [CWE- 23] in FortiWeb version 7.0.1 and below, 6.4 all versions, 6.3 all versions, 6.2 all versions may allow an authenticated user to obtain unauthorized access to files and data via specifically crafted web requests. CVE ID : CVE-2023- 23778	https://fortig uard.com/psir t/FG-IR-22- 142	A-FOR-FORT- 160323/201

0-1

1-2

2-33-44-5Page 107 of 859

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Vers	Affected Version(s): From (including) 6.3.6 Up to (excluding) 6.3.21							
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	6.5	A relative path traversal in Fortinet FortiWeb version 7.0.0 through 7.0.2, FortiWeb version 6.3.6 through 6.3.20, FortiWeb 6.4 all versions allows attacker to information disclosure via specially crafted web requests. CVE ID : CVE-2023- 23784	https://fortig uard.com/psir t/FG-IR-22- 251	A-FOR-FORT- 160323/202			
Affected Vers	sion(s): From (i	ncluding)	6.3.6 Up to (including)	6.3.19				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	Multiple improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below may allow an authenticated attacker to execute unauthorized code or commands via crafted parameters of HTTP requests. CVE ID : CVE-2023- 23779	N/A	A-FOR-FORT- 160323/203			
Affected Vers	Affected Version(s): From (including) 6.3.6 Up to (including) 6.3.21							
N/A	27-Feb-2023	3.3	An unauthorized configuration download	https://fortig uard.com/psir	A-FOR-FORT- 160323/204			
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in FortiWeb 6.3.6 through 6.3.21, 6.4.0 through 6.4.2 and 7.0.0 through 7.0.4 may allow a local attacker to access confidential configuration files via a crafted http request. CVE ID : CVE-2023- 22636	t/FG-IR-22- 460	
Affected Ver	sion(s): From (i	ncluding)	6.4.0 Up to (excluding)	6.4.2	
Use of Externally- Controlled Format String	16-Feb-2023	7.8	A use of externally- controlled format string in Fortinet FortiWeb version 7.0.0 through 7.0.1, FortiWeb 6.4 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments. CVE ID : CVE-2023- 23783	https://fortig uard.com/psir t/FG-IR-22- 187	A-FOR-FORT- 160323/205
Affected Ver	sion(s): From (i	ncluding)	6.4.0 Up to (including)	6.4.2	
Out-of- bounds Write	16-Feb-2023	8.8	A stack-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, Fortinet FortiWeb version 6.3.6 through 6.3.19, Fortinet FortiWeb 6.4 all versions allows attacker to escalation of privilege via	https://fortig uard.com/psir t/FG-IR-22- 118	A-FOR-FORT- 160323/206

0-1

1-2

2-33-44-5Page 109 of 859

5-6

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specifically crafted HTTP requests. CVE ID : CVE-2023- 23780		
Out-of- bounds Write	16-Feb-2023	8.8	A stack-based buffer overflow vulnerability [CWE- 121] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below SAML server configuration may allow an authenticated attacker to achieve arbitrary code execution via specifically crafted XML files. CVE ID : CVE-2023- 23781	https://fortig uard.com/psir t/FG-IR-22- 151	A-FOR-FORT- 160323/207
Out-of- bounds Write	16-Feb-2023	7.8	A heap-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, FortiWeb version 6.3.0 through 6.3.19, FortiWeb 6.4 all versions, FortiWeb 6.2 all versions, FortiWeb 6.1 all versions allows attacker to escalation of privilege via specifically crafted arguments to existing commands. CVE ID : CVE-2023- 23782	https://fortig uard.com/psir t/FG-IR-22- 111	A-FOR-FORT- 160323/208

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	16-Feb-2023	7.8	A stack-based buffer overflow in Fortinet FortiWeb 6.4 all versions, FortiWeb versions 6.3.17 and earlier, FortiWeb versions 6.2.6 and earlier, FortiWeb versions 6.1.2 and earlier, FortiWeb versions 6.0.7 and earlier, FortiWeb versions 5.9.1 and earlier, FortiWeb 5.8 all versions, FortiWeb 5.7 all versions, FortiWeb 5.6 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments. CVE ID : CVE-2023- 25602	https://fortig uard.com/psir t/FG-IR-21- 234	A-FOR-FORT- 160323/209
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	6.5	A relative path traversal in Fortinet FortiWeb version 7.0.0 through 7.0.2, FortiWeb version 6.3.6 through 6.3.20, FortiWeb 6.4 all versions allows attacker to information disclosure via specially crafted web requests. CVE ID : CVE-2023- 23784	https://fortig uard.com/psir t/FG-IR-22- 251	A-FOR-FORT- 160323/210

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Feb-2023	3.3	An unauthorized configuration download vulnerability in FortiWeb 6.3.6 through 6.3.21, 6.4.0 through 6.4.2 and 7.0.0 through 7.0.4 may allow a local attacker to access confidential configuration files via a crafted http request. CVE ID : CVE-2023-	https://fortig uard.com/psir t/FG-IR-22- 460	A-FOR-FORT- 160323/211
			22636		
Affected Ver	sion(s): From (i	ncluding)	7.0.0 Up to (excluding)	7.0.2	
Out-of- bounds Write	16-Feb-2023	8.8	A stack-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, Fortinet FortiWeb version 6.3.6 through 6.3.19, Fortinet FortiWeb 6.4 all versions allows attacker to escalation of privilege via specifically crafted HTTP requests. CVE ID : CVE-2023-	https://fortig uard.com/psir t/FG-IR-22- 118	A-FOR-FORT- 160323/212
			23780		
Out-of- bounds Write	16-Feb-2023	8.8	A stack-based buffer overflow vulnerability [CWE- 121] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below SAML server	https://fortig uard.com/psir t/FG-IR-22- 151	A-FOR-FORT- 160323/213

0-1

1-2

2-33-44-5Page 112 of 859

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration may allow an authenticated attacker to achieve arbitrary code execution via specifically crafted XML files. CVE ID : CVE-2023- 23781		
Out-of- bounds Write	16-Feb-2023	7.8	A heap-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, FortiWeb version 6.3.0 through 6.3.19, FortiWeb 6.4 all versions, FortiWeb 6.2 all versions, FortiWeb 6.1 all versions allows attacker to escalation of privilege via specifically crafted arguments to existing commands. CVE ID : CVE-2023- 23782	https://fortig uard.com/psir t/FG-IR-22- 111	A-FOR-FORT- 160323/214
Use of Externally- Controlled Format String	16-Feb-2023	7.8	A use of externally- controlled format string in Fortinet FortiWeb version 7.0.0 through 7.0.1, FortiWeb 6.4 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments.	https://fortig uard.com/psir t/FG-IR-22- 187	A-FOR-FORT- 160323/215

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23783		
Affected Vers	sion(s): From (i	ncluding)	7.0.0 Up to (excluding)	7.0.3	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	uard com/nsi			A-FOR-FORT- 160323/216
Affected Vers	sion(s): From (i	ncluding)	7.0.0 Up to (including)	7.0.4	
N/A	27-Feb-2023	3.3	An unauthorized configuration download vulnerability in FortiWeb 6.3.6 through 6.3.21, 6.4.0 through 6.4.2 and 7.0.0 through 7.0.4 may allow a local attacker to access confidential configuration files via a crafted http request. CVE ID : CVE-2023- 22636	https://fortig uard.com/psir t/FG-IR-22- 460	A-FOR-FORT- 160323/217
Vendor: fraj					
Product: for	-				
	sion(s): * Up to	(excluding			
Improper Neutralizat ion of	26-Feb-2023	6.1	The frp_form_answers (aka Forms Export)	https://typo3. org/security/ advisory/typo	A-FRA-FORM- 160323/218
CVSS Scoring S	icale 0-1	1-2 2	-3 3-4 4-5 5 Page 114 of 859	-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			extension before 3.1.2, and 4.x before 4.0.2, for TYPO3 allows XSS via saved emails.	3-ext-sa- 2023-002, https://typo3. org/help/secu rity-advisories	
			CVE ID : CVE-2023- 26091		
Affected Ver	sion(s): From (i	ncluding)	4.0.0 Up to (excluding)	4.0.2	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	26-Feb-2023	6.1	The frp_form_answers (aka Forms Export) extension before 3.1.2, and 4.x before 4.0.2, for TYPO3 allows XSS via saved emails. CVE ID : CVE-2023- 26091	https://typo3. org/security/ advisory/typo 3-ext-sa- 2023-002, https://typo3. org/help/secu rity-advisories	A-FRA-FORM- 160323/219
Vendor: Fro	oxlor			•	
Product: fro	oxlor				
Affected Ver	sion(s): * Up to	(excluding	g) 2.0.11		
Improper Control of Generation of Code ('Code Injection')	17-Feb-2023	8.8	Code Injection in GitHub repository froxlor/froxlor prior to 2.0.11. CVE ID : CVE-2023- 0877	https://huntr. dev/bounties/ b29cf038- 06f1-4fb0- 9437- 08f2991f92a8 , https://github .com/froxlor/f roxlor/commi t/aa48ffca2bc af7ae57be3b8 147bb3138ab dab984	A-FRO-FROX- 160323/220
Cross-Site Request Forgery (CSRF)	25-Feb-2023	8.8	Cross-Site Request Forgery (CSRF) in GitHub repository froxlor/froxlor prior to 2.0.11.	https://huntr. dev/bounties/ ba3cd929- 8b60-4d8d- b77d- f28409ecf387,	A-FRO-FROX- 160323/221

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- https://github 1033 .com/froxlor/f roxlor/commi t/4003a8d2b 60728a77476 d1d4f5aa5c63 5f128950 5f128950		
Vendor: GE				•	
Product: dig	gital_industria	l_gateway	_server		
Affected Vers	sion(s): * Up to	(including	g) 7.612		
Integer Overflow or Wraparoun d	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code. CVE ID : CVE-2023- 0754	N/A	A-GE-DIGI- 160323/222
Improper Validation of Array Index	23-Feb-2023	9.8	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code. CVE ID : CVE-2023- 0755	N/A	A-GE-DIGI- 160323/223
Vendor: Ger	netechsolution	S			
Product: pie	e_register				
Affected Ver	sion(s): * Up to	(excluding	g) 3.8.2.3		
URL Redirectio n to	27-Feb-2023	5.4	The Registration Forms WordPress plugin before 3.8.2.3	N/A	A-GEN-PIE 160323/224

 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
Untrusted Site ('Open Redirect')		does not properly validate the redirection URL when logging in and login out, leading to an Open Redirect vulnerability CVE ID : CVE-2023- 0552			
Vendor: Ge	ntoo		0332		
Product: so					
Affected Ver	sion(s): * Up to	(excluding	g) 1.0.1		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	9.1	Gentoo soko is the code that powers packages.gentoo.org. Versions prior to 1.0.1 are vulnerable to SQL Injection, leading to a Denial of Service. If the user selects (in user preferences) the "Recently Visited Packages" view for the index page, the value of the `search_history` cookie is used as a base64 encoded comma separated list of atoms. These are string loaded directly into the SQL query with `atom = '%s'` format string. As a result, any user can modify the browser's cookie value and inject most SQL queries. A proof of concept malformed cookie was	https://gitwe b.gentoo.org/s ites/soko.git/ commit/?id=5 ae9ca83b735 804f2bd4055 92983a73d7fc c42f4, https://github .com/gentoo/ soko/security /advisories/G HSA-gp8g- jfq9-5q2g	A-GEN-SOKO- 160323/225

0-1

1-2

2-3

3-4 4-5 Page **117** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			generated that wiped					
			the database or					
			changed it's content.					
			On the database,					
			only public data is					
			stored, so there is no					
			confidentiality issues					
			to site users. If it is					
			known that the					
			database was					
			modified, a full					
			restoration of data is					
			possible by					
			performing a full					
			database wipe and					
			performing full					
			update of all					
			components. This					
			issue is patched with					
			commit id					
			5ae9ca83b73.					
			Version 1.0.1					
			contains the patch. If					
			users are unable to					
			upgrade					
			immediately, the					
			following					
			workarounds may be					
			applied: (1.) Use a					
			proxy to always drop					
			the `search_history` cookie until					
			upgraded. The					
			impact on user					
			experience is low.					
			(2.) Sanitize to the					
			value of					
			`search_history`					
			cookie after base64					
			decoding it.					
			_					
			CVE ID : CVE-2023-					
			26033					
Vendor: geo	otools							

0-1

1-2

2-33-44-5Page 118 of 859

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Product: geotools								
Affected Version(s): * Up to (excluding) 24.7								
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoTools is an open source Java library that provides tools for geospatial data. GeoTools includes support for OGC Filter expression language parsing, encoding and execution against a range of datastore. SQL Injection Vulnerabilities have been found when executing OGC Filters with JDBCDataStore implementations. Users are advised to upgrade to either version 27.4 or to 28.2 to resolve this issue. Users unable to upgrade may disable `encode functions` for PostGIS DataStores or enable `prepared statements` for JDBCDataStores as a partial mitigation. CVE ID : CVE-2023- 25158	https://github .com/geotools /geotools/co mmit/64fb4c 47f43ca818c2 fe96a94651bf f1b3b3ed2b, https://github .com/geotools /geotools/sec urity/advisori es/GHSA- 99c3-qc2q- p94m	A-GEO-GEOT- 160323/226			
	sion(s): From (i	ncluding)	25.0 Up to (excluding)	1				
Improper Neutralizat ion of Special Elements used in an	21-Feb-2023	9.8	GeoTools is an open source Java library that provides tools for geospatial data. GeoTools includes support for OGC	https://github .com/geotools /geotools/co mmit/64fb4c 47f43ca818c2 fe96a94651bf	A-GEO-GEOT- 160323/227			

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			Filter expression language parsing, encoding and execution against a range of datastore. SQL Injection Vulnerabilities have been found when executing OGC Filters with JDBCDataStore implementations. Users are advised to upgrade to either version 27.4 or to 28.2 to resolve this issue. Users unable to upgrade may disable `encode functions` for PostGIS DataStores or enable `prepared statements` for JDBCDataStores as a partial mitigation. CVE ID : CVE-2023- 25158	https://github .com/geotools /geotools/sec urity/advisori es/GHSA- 99c3-qc2q- p94m 99c3-qc2q- p94m 99c3-qc2q- p94m	
Affected Ver	sion(s): From (i	ncluding)	26.0 Up to (excluding)	26.7	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoTools is an open source Java library that provides tools for geospatial data. GeoTools includes support for OGC Filter expression language parsing, encoding and execution against a range of datastore. SQL Injection Vulnerabilities have been found when executing OGC	https://github .com/geotools /geotools/co mmit/64fb4c 47f43ca818c2 fe96a94651bf f1b3b3ed2b, https://github .com/geotools /geotools/sec urity/advisori es/GHSA- 99c3-qc2q- p94m	A-GEO-GEOT- 160323/228

0-1

1-2

2-3

3-4 4-5 Page **120** of **859** 6-7

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
	Filters withJDBCDataStoreimplementations.Users are advised toupgrade to eitherversion 27.4 or to28.2 to resolve thisissue. Users unableto upgrade maydisable `encodefunctions` forPostGIS DataStoresor enable `preparedstatements` forJDBCDataStores as apartial mitigation.CVE ID : CVE-2023-				
			25158		
Affected Ver	sion(s): From (i	ncluding)	27.0 Up to (excluding)	27.4	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoTools is an open source Java library that provides tools for geospatial data. GeoTools includes support for OGC Filter expression language parsing, encoding and execution against a range of datastore. SQL Injection Vulnerabilities have been found when executing OGC Filters with JDBCDataStore implementations. Users are advised to upgrade to either version 27.4 or to 28.2 to resolve this issue. Users unable to upgrade may	https://github .com/geotools /geotools/co mmit/64fb4c 47f43ca818c2 fe96a94651bf f1b3b3ed2b, https://github .com/geotools /geotools/sec urity/advisori es/GHSA- 99c3-qc2q- p94m	A-GEO-GEOT- 160323/229

0-1

1-2

2-3 3-4 4-5 Page **121** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disable `encode functions` for PostGIS DataStores or enable `prepared statements` for JDBCDataStores as a partial mitigation. CVE ID : CVE-2023- 25158		
Affected Ver	sion(s): From (i	ncluding)	28.0 Up to (excluding)	28.2	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoTools is an open source Java library that provides tools for geospatial data. GeoTools includes support for OGC Filter expression language parsing, encoding and execution against a range of datastore. SQL Injection Vulnerabilities have been found when executing OGC Filters with JDBCDataStore implementations. Users are advised to upgrade to either version 27.4 or to 28.2 to resolve this issue. Users unable to upgrade may disable `encode functions` for PostGIS DataStores or enable `prepared statements` for JDBCDataStores as a partial mitigation.	https://github .com/geotools /geotools/co mmit/64fb4c 47f43ca818c2 fe96a94651bf f1b3b3ed2b, https://github .com/geotools /geotools/sec urity/advisori es/GHSA- 99c3-qc2q- p94m	A-GEO-GEOT- 160323/230

0-1

1-2

2-3

3-4 4-5 Page **122** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID		
			CVE ID : CVE-2023- 25158		
Vendor: Git	hub				
Product: en	terprise_serve	r			
Affected Ver	sion(s): From (i	ncluding)	3.7.0 Up to (excluding)	3.7.6	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	6.5	A path traversal vulnerability was identified in GitHub Enterprise Server that allowed arbitrary file reading when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.7.6. This vulnerability was reported via the GitHub Bug Bounty program. CVE ID : CVE-2023- 22380	https://docs.g ithub.com/en /enterprise- server@3.7/a dmin/release- notes#3.7.6	A-GIT-ENTE- 160323/231
Product: glu	ısterfs				
Affected Ver	sion(s): 11.0				
Out-of- bounds Read	21-Feb-2023	7.5	In Gluster GlusterFS 11.0, there is an xlators/mount/fuse/ src/fuse-bridge.c	https://github .com/gluster/ glusterfs/issu es/3954	A-GLU-GLUS- 160323/232

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		
			notify stack-based buffer over-read. CVE ID : CVE-2023-				
			26253				
Vendor: Gno							
Product: ep							
Affected Vers	sion(s): * Up to	(excluding		Γ	Γ		
Exposure of Resource to Wrong Sphere	20-Feb-2023	7.5	In Epiphany (aka GNOME Web) through 43.0, untrusted web content can trick users into exfiltrating passwords, because autofill occurs in sandboxed contexts.	https://gitlab. gnome.org/G NOME/epipha ny/- /merge_reque sts/1275	A-GNO-EPIP- 160323/233		
			CVE ID : CVE-2023- 26081				
Vendor: gnp	oublisher						
Product: gn	_publisher						
Affected Vers	sion(s): * Up to	(including	g) 1.5.5				
Improper Neutralizat ion of Input During28-Feb-20236.1The GN Publisher plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in versions up to, and including, 1.5.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick aN/AA-GNP-GN_P- 160323/234							
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10		

Page 124 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user into performing an action such as clicking on a link. CVE ID : CVE-2023- 1080		
Vendor: GN	U				
Product: libmicrohttpd					
Affected Version(s): * Up to (excluding) 0.9.76					
Out-of- bounds Read	28-Feb-2023	7.5	GNU libmicrohttpd before 0.9.76 allows remote DoS (Denial of Service) due to improper parsing of a multipart/form- data boundary in the postprocessor.c MHD_create_post_pr ocessor() method. This allows an attacker to remotely send a malicious HTTP POST packet that includes one or more '\0' bytes in a multipart/form-data boundary field, which - assuming a specific heap layout - will result in an out- of-bounds read and a crash in the find_boundary() function. CVE ID : CVE-2023- 27371	https://git.gn unet.org/libm icrohttpd.git/c ommit/?id=6d 6846e20bfdf4 b3eb1b592c9 7520a532f72 4238	A-GNU-LIBM- 160323/235
Vendor: go-redrock Product: tutortrac					
Affected Version(s): * Up to (excluding) 4.2.170210					
Improper Neutralizat ion of	21-Feb-2023	5.4	Multiple stored cross-site scripting (XSS) vulnerabilities	N/A	A-GOTUTO- 160323/236
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 125 of 859					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			in Redrock Software TutorTrac before v4.2.170210 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the reason and location fields of the visits listing page. CVE ID : CVE-2023- 24081		
Vendor: Go	ogle			I	
Product: ch	rome				
Affected Ver	sion(s): * Up to	(excluding	g) 110.0.5481.177		
Use After Free	22-Feb-2023	8.8	Use after free in Web Payments API in Google Chrome on Android prior to 110.0.5481.177 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) CVE ID : CVE-2023-	https://chrom ereleases.goog leblog.com/20 23/02/stable- channel- desktop- update_22.ht ml	A-GOO-CHRO- 160323/237
Use After Free	22-Feb-2023	8.8	0927 Use after free in SwiftShader in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	https://chrom ereleases.goog leblog.com/20 23/02/stable- channel- desktop- update_22.ht ml	A-GOO-CHRO- 160323/238

0-1

1-2

2-3

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Chromium security severity: High)		
			CVE ID : CVE-2023- 0928		
Use After Free	r 22-Feb-2023 8.8 Potentially heap correction of the correct of th		Use after free in Vulkan in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	https://chrom ereleases.goog leblog.com/20 23/02/stable- channel- desktop- update_22.ht ml	A-GOO-CHRO- 160323/239
			CVE ID : CVE-2023- 0929		
Out-of- bounds Write	22-Feb-2023	8.8	Heap buffer overflow in Video in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) CVE ID : CVE-2023- 0930	https://chrom ereleases.goog leblog.com/20 23/02/stable- channel- desktop- update_22.ht ml	A-GOO-CHRO- 160323/240
Use After Free	22-Feb-2023	8.8	Use after free in Video in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	https://chrom ereleases.goog leblog.com/20 23/02/stable- channel- desktop- update_22.ht ml	A-GOO-CHRO- 160323/241

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 0931		
Use After Free	22-Feb-2023	8.8	Use after free in WebRTC in Google Chrome on Windows prior to 110.0.5481.177 allowed a remote attacker who convinced the user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) CVE ID : CVE-2023-	https://chrom ereleases.goog leblog.com/20 23/02/stable- channel- desktop- update_22.ht ml	A-GOO-CHRO- 160323/242
			0932		
Integer Overflow or Wraparoun d	22-Feb-2023	8.8	Integer overflow in PDF in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium)	https://chrom ereleases.goog leblog.com/20 23/02/stable- channel- desktop- update_22.ht ml	A-GOO-CHRO- 160323/243
			CVE ID : CVE-2023- 0933		
Use After Free	22-Feb-2023	8.8	Use after free in Prompts in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	https://chrom ereleases.goog leblog.com/20 23/02/stable- channel- desktop- update_22.ht ml	A-GOO-CHRO- 160323/244

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Chromium security severity: Critical) CVE ID : CVE-2023-		
			0941		
Vendor: gpa					
Product: gp		(I]]			
Affected Ver	sion(s): * Up to	(including	g) 2.2.0		[
Heap- based Buffer Overflow	16-Feb-2023	7.8	Heap-based Buffer Overflow in GitHub repository gpac/gpac prior to 2.3.0-DEV. CVE ID : CVE-2023- 0866	https://huntr. dev/bounties/ 7d3c5792- d20b-4cb6- 9c6d- bb14f3430d7f , https://github .com/gpac/gp ac/commit/b9 64fe4226f142 4cf676d5822e f898b6b01f59 37	A-GPA-GPAC- 160323/245
Vendor: gra	dio_project				
Product: gra					
Affected Ver	sion(s): * Up to	(excluding		I	Γ
Use of Hard- coded Credentials	23-Feb-2023	9.8	Gradio is an open- source Python library to build machine learning and data science demos and web applications. Versions prior to 3.13.1 contain Use of Hard-coded Credentials. When using Gradio's share links (i.e. creating a Gradio app and then setting `share=True`), a private SSH key is	https://github .com/gradio- app/gradio/se curity/advisor ies/GHSA- 3x5j-9vwr- 8rr5	A-GRA-GRAD- 160323/246

0-1

1-2

2-33-44-5Page 129 of 859

6-7

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to any user that connects to the Gradio machine, which means that a user could access other users' shared Gradio demos. From there, other exploits are possible depending on the level of access/exposure the Gradio app provides. This issue is patched in version 3.13.1, however, users are recommended to update to 3.19.1 or later where the FRP solution has been properly tested. CVE ID : CVE-2023- 25823		
Vendor: gre	enshiftwp				
Product: gro	eenshiftanin	nation_an	d_page_builder_block	S	
Affected Ver	sion(s): * Up to	(excluding			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The Greenshift WordPress plugin before 5.0 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	N/A	A-GRE-GREE- 160323/247

0-1

1-2

2-33-44-5Page 130 of 859

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 0378		
Vendor: gsp	olugins				
Product: gs	_books_showca	ise			
Affected Ver	sion(s): * Up to	(excluding	g) 1.3.1		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The GS Books Showcase WordPress plugin before 1.3.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. CVE ID : CVE-2023- 0541	N/A	A-GSP-GS_B- 160323/248
Product: gs	_filterable_por	tfolio			
Affected Ver	sion(s): * Up to	(excluding	g) 1.6.1		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The GS Filterable Portfolio WordPress plugin before 1.6.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform	N/A	A-GSP-GS_F- 160323/249

0-1

1-2

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Stored Cross-Site Scripting attacks. CVE ID : CVE-2023- 0540		
Product: gs	_insever_portfo	olio			
Affected Ver	sion(s): * Up to	(excluding	g) 1.4.5		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	The GS Insever Portfolio WordPress plugin before 1.4.5 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. CVE ID : CVE-2023- 0539	N/A	A-GSP-GS_I- 160323/250
Product: gs	_portfolio_for_o	envato		I	
Affected Ver	sion(s): * Up to	(excluding	g) 1.4.0	-	_
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The GS Portfolio for Envato WordPress plugin before 1.4.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embedded, which could allow users with the contributor role and above to perform Stored	N/A	A-GSP-GS_P- 160323/251

0-1

1-2

2-3

3-4 4-5 Page **132** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	De	escriptio	n & CVE	ID		Patch			NCIIP	CID
			atta	acks E ID : C	Scriptin VE-202	0						
Product: gs	Product: gs_products_slider											
Affected Ver	sion(s): * Up to	(excludin	g) 1.	5.9			-					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	Slic Wo bef val: son attr bac wh is e cou wit role per Cro atta	ore 1.5. idate an ne of its ributes putting ck in a p ere the mbed, w ild allow ch the co e and al form St oss-Site acks E ID : C	nerce s plugin 9 does r ad escap s shortco before them age/pos shortco which v users ontribut	e ode st de or	N/A	Ą			SP-GS)323/	_
Vendor: has	hicorp						L					
Product: go	-getter											
Affected Ver	sion(s): * Up to	(includin	g) 1.6	5.2								
N/A 16-Feb-2023 6.5 HashiCorp go-getter up to 1.6.2 and 2.1.1 is vulnerable to decompression bombs. Fixed in 1.7.0 and 2.2.0. CVE ID : CVE-2023- 0475			.1 7.0	s.ha m/t 202 gett vuli den ser mai con	os://dis ashicorp t/hcsec 23-4-go- ter- nerable ial-of- vice-via licious- npresse hive/50	p.co - - -to- -		IAS-G 0323/				
CVSS Scoring S	Scale 0-1	1-2 2	2-3	3-4	4-5	5	-6	6-7	7-8	3	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 2.1.1	L			
N/A	16-Feb-2023	6.5	HashiCorp go-getter up to 1.6.2 and 2.1.1 is vulnerable to decompression bombs. Fixed in 1.7.0 and 2.2.0. CVE ID : CVE-2023- 0475	https://discus s.hashicorp.co m/t/hcsec- 2023-4-go- getter- vulnerable-to- denial-of- service-via- malicious- compressed- archive/5012 5	A-HAS-GO-G- 160323/254
Product: no	mad sion(s): * Up to	(excluding	n) 1 2 15		
Allected ver		Cexcluding	[
N/A	16-Feb-2023	6.5	HashiCorp Nomad and Nomad Enterprise 1.2.15 up to 1.3.8, and 1.4.3 jobs using a maliciously compressed artifact stanza source can cause excessive disk usage. Fixed in 1.2.16, 1.3.9, and 1.4.4. CVE ID : CVE-2023- 0821	https://discus s.hashicorp.co m/t/hcsec- 2023-05- nomad-client- vulnerable-to- decompressio n-bombs-in- artifact- block/50292	A-HAS-NOMA- 160323/255
Affected Ver	sion(s): From (i	ncluding)	1.3.0 Up to (excluding)	1.3.9	
N/A	16-Feb-2023	6.5	HashiCorp Nomad and Nomad Enterprise 1.2.15 up to 1.3.8, and 1.4.3 jobs using a maliciously compressed artifact stanza source can cause excessive disk usage. Fixed in	https://discus s.hashicorp.co m/t/hcsec- 2023-05- nomad-client- vulnerable-to- decompressio n-bombs-in- artifact- block/50292	A-HAS-NOMA- 160323/256

0-1

1-2

2-33-44-5Page 134 of 859

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			1.2.16, 1.3.9, and 1.4.4.					
			CVE ID : CVE-2023-					
			0821					
Affected Version(s): From (including) 1.4.0 Up to (excluding) 1.4.4								
N/A	16-Feb-2023	6.5	HashiCorp Nomad and Nomad Enterprise 1.2.15 up to 1.3.8, and 1.4.3 jobs using a maliciously compressed artifact stanza source can cause excessive disk usage. Fixed in 1.2.16, 1.3.9, and 1.4.4. CVE ID : CVE-2023- 0921	https://discus s.hashicorp.co m/t/hcsec- 2023-05- nomad-client- vulnerable-to- decompressio n-bombs-in- artifact- block/50292	A-HAS-NOMA- 160323/257			
** 1 1			0821					
Vendor: has		~ ~						
	tensions_for_cl							
Affected Vers	sion(s): * Up to	(excluding			Γ			
Cross-Site Request Forgery (CSRF)	17-Feb-2023	4.3	Cross-Site Request Forgery (CSRF) vulnerability in HasThemes Extensions For CF7 plugin <= 2.0.8 versions leads to arbitrary plugin activation.	N/A	A-HAS-EXTE- 160323/258			
			CVE ID : CVE-2023- 23899					
Product: sh	oplentor							
Affected Version(s): * Up to (excluding) 2.5.4								
Deserializa tion of Untrusted Data	21-Feb-2023	9.8	The ShopLentor WordPress plugin before 2.5.4 unserializes user input from cookies in	https://plugin s.trac.wordpre ss.org/change set/2852711/ woolentor-	A-HAS-SHOP- 160323/259			
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-44-555	-6 6-7 7-8	8 8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to track viewed products and user data, which could lead to PHP Object Injection. CVE ID : CVE-2023- 0232	addons/trunk /includes/hel per- function.php	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The ShopLentor WordPress plugin before 2.5.4 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. CVE ID : CVE-2023- 0231	N/A	A-HAS-SHOP- 160323/260
Vendor: Hay					
Product: cu		1 1: >			
Affected Vers	sion(s): From (i	ncluding)	7.57.0 Up to (excluding	() 7.88.0	1
Allocation of Resources Without Limits or Throttling 23-Feb-2023 7.5 7.5 7.5 7.5 7.5 7.5 7.5 7.5 7.5		An allocation of resources without limits or throttling vulnerability exists in curl <v7.88.0 based on the "chained" HTTP compression algorithms, meaning that a server response can be compressed multiple times and potentially with</v7.88.0 	https://securi ty.netapp.com /advisory/nta p-20230309- 0006/	A-HAX-CURL- 160323/261	
			differentalgorithms.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The number of acceptable "links" in this "decompression chain" wascapped, but the cap was implemented on a per-header basis allowing a maliciousserver to insert a virtually unlimited number of compression steps simply byusing many headers. The use of such a decompression chain could result in a "malloc bomb", making curl end up spending enormous amounts of allocated heap memory, or trying to and returning out of memory errors. CVE ID : CVE-2023-		
Affected Mer		u alu din a)	23916		
Affected Ver	sion(s): From (i	ncluding)	7.77.0 Up to (excluding	J 7.88.0	
Cleartext Transmissi on of Sensitive Informatio n	23-Feb-2023	9.1	A cleartext transmission of sensitive information vulnerability exists in curl <v7.88.0 that<br="">could cause HSTS functionality fail when multiple URLs are requested serially. Using its HSTS support, curl can be instructed to use HTTPS instead of usingan insecure clear-text HTTP step</v7.88.0>	https://securi ty.netapp.com /advisory/nta p-20230309- 0006/	A-HAX-CURL- 160323/262

0-1

1-2

2-33-44-5Page 137 of 859

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			even when HTTP is provided in the URL. ThisHSTS mechanism would however surprisingly be ignored by subsequent transferswhen done on the same command line because the state would not be properlycarried on. CVE ID : CVE-2023- 23914		
Cleartext Transmissi on of Sensitive Informatio n	23-Feb-2023	6.5	A cleartext transmission of sensitive information vulnerability exists in curl <v7.88.0 that<br="">could cause HSTS functionality to behave incorrectly when multiple URLs are requested in parallel. Using its HSTS support, curl can be instructed to use HTTPS instead of using an insecure clear-text HTTP step even when HTTP is provided in the URL. This HSTS mechanism would however surprisingly fail when multiple transfers are done in parallel as the HSTS cache file gets overwritten by the</v7.88.0>	https://securi ty.netapp.com /advisory/nta p-20230309- 0006/	A-HAX-CURL- 160323/263

0-1

1-2

2-33-44-5Page 138 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			most recentlycompleted transfer. A later HTTP-only transfer to the earlier host name would then *not* get upgraded properly to HSTS. CVE ID : CVE-2023- 23915		
	ır_of_code_pyt <mark>ur_of_code_pyt</mark>				
	sion(s): 2015-1		5		
N/A	22-Feb-2023	9.8	hour_of_code_python _2015 commit 520929797b9ca43b b818b2e8f963fb202 5459fa3 was discovered to contain a code execution backdoor via the request package (requirements.txt). This vulnerability allows attackers to access sensitive user information and execute arbitrary code. CVE ID : CVE-2023- 24107	N/A	A-HOU-HOUR- 160323/264
Vendor: IBM					
Product: asp					
	sion(s): * Up to	(including			
Improper Neutralizat ion of Input During Web Page	17-Feb-2023	5.4	IBM Aspera Faspex 4.4.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary	https://www.i bm.com/supp ort/pages/no de/6952319, https://excha nge.xforce.ibm	A-IBM-ASPE- 160323/265
CVSS Scoring S	Scale 0-1	1-2 2	- 3 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244117. CVE ID : CVE-2023- 22868	cloud.com/vul nerabilities/2 44117	
Affected Ver	sion(s): 4.4.1			L	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	5.4	IBM Aspera Faspex 4.4.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244117. CVE ID : CVE-2023-	https://www.i bm.com/supp ort/pages/no de/6952319, https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 44117	A-IBM-ASPE- 160323/266
			22868		
	oud_pak_for_bu	isiness_a	utomation		
Allected ver	31011(3): 10.0.0		IBM Cloud Pak for		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 44100, https://www.i bm.com/supp ort/pages/no de/6958062	A-IBM-CLOU- 160323/267
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10

Page 140 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. CVE ID : CVE-2023- 22860				
Affected Ver	sion(s): 18.0.2		22000				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. CVE ID : CVE-2023- 22860	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 44100, https://www.i bm.com/supp ort/pages/no de/6958062	A-IBM-CLOU- 160323/268		
Affected Version(s): 19.0.1							
Improper Neutralizat ion of Input During	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3,	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 44100,	A-IBM-CLOU- 160323/269		

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100.	https://www.i bm.com/supp ort/pages/no de/6958062	
			CVE ID : CVE-2023- 22860		
Affected Ver	sion(s): 19.0.3				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. CVE ID : CVE-2023- 22860	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 44100, https://www.i bm.com/supp ort/pages/no de/6958062	A-IBM-CLOU- 160323/270

0-1

1-2

2-33-44-5Page 142 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 20.0.1				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. CVE ID : CVE-2023-	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 44100, https://www.i bm.com/supp ort/pages/no de/6958062	A-IBM-CLOU- 160323/271
			22860		
Affected Ver	sion(s): 20.0.3				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 44100, https://www.i bm.com/supp ort/pages/no de/6958062	A-IBM-CLOU- 160323/272

0-1

1-2

2-3

3-4 4-5 Page **143** of **859** 6-7

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure within a trusted session. IBM X-Force ID: 244100.		
			CVE ID : CVE-2023- 22860		
Affected Ver	sion(s): 21.0.1				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. CVE ID : CVE-2023- 22860	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 44100, https://www.i bm.com/supp ort/pages/no de/6958062	A-IBM-CLOU- 160323/273
Affected Ver	sion(s): 21.0.2			1	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 44100, https://www.i bm.com/supp ort/pages/no de/6958062	A-IBM-CLOU- 160323/274

0-1

1-2

2-33-44-5Page 144 of 859

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. CVE ID : CVE-2023- 22860					
Affected Ver	sion(s): 21.0.3							
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. CVE ID : CVE-2023- 22860	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 44100, https://www.i bm.com/supp ort/pages/no de/6958062	A-IBM-CLOU- 160323/275			
	Affected Version(s): 22.0.1							
Improper Neutralizat ion of Input During Web Page	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3,	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 44100, https://www.i	A-IBM-CLOU- 160323/276			

0-1

1-2

5-6

6-7

7-8

0-1

1-2

2-3

3-4 4-5 Page **146** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 11.7				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Feb-2023	7.5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (//) to view arbitrary files on the system. IBM X-Force ID: 246333 CVE ID : CVE-2023- 24960	https://www.i bm.com/supp ort/pages/no de/6953521, https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 46333	A-IBM-INFO- 160323/278
Cleartext Storage of Sensitive Informatio n	17-Feb-2023	5.5	IBM InfoSphere Information Server 11.7 could allow a local user to obtain sensitive information from a log files. IBM X-Force ID: 246463. CVE ID : CVE-2023- 24964	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 46463, https://www.i bm.com/supp ort/pages/no de/6953519	A-IBM-INFO- 160323/279
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247646.	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 47646, https://www.i bm.com/supp ort/pages/no de/6956598	A-IBM-INFO- 160323/280

0-1

1-2

2-3

3-4 4-5 Page **147** of **859** 6-7 7-8

5-6

Product: jd-gu	ui		CVE ID : CVE-2023- 25928							
Product: jd-gu	ui									
Affected Versio			Vendor: jd-gui_project							
	on(s): 1.6.6									
Deserializa tion of Untrusted Data	21-Feb-2023	9.8	JD-GUI 1.6.6 allows deserialization via UIMainWindowPrefe rencesProvider.singl eInstance. CVE ID : CVE-2023- 26234	N/A	A-JDJD-G- 160323/281					
ImproperNeutralization ofInputDuringWeb PageGeneration('Cross-siteScripting')	21-Feb-2023	6.1	JD-GUI 1.6.6 allows XSS via util/net/InterProces sCommunicationUtil. java. CVE ID : CVE-2023- 26235	https://github .com/java- decompiler/jd -gui/pull/418	A-JDJD-G- 160323/282					
Vendor: Joom	ıla									
Product: joon	nla\!									
Affected Version	on(s): From (i	ncluding)	4.0.0 Up to (including)	4.2.7						
N/A 1	16-Feb-2023	5.3	An issue was discovered in Joomla! 4.0.0 through 4.2.7. An improper access check allows unauthorized access to webservice endpoints. CVE ID : CVE-2023- 23752	https://devel oper.joomla.or g/security- centre/894- 20230201- core- improper- access-check- in- webservice- endpoints.htm l	A-JOO-JOOM- 160323/283					
Vendor: joomunited										
Product: wp_1	meta_seo									
Affected Version	on(s): * Up to	(including	;) 4.5.3							

0-1

1-2

2-3

3-4 4-5 Page **148** of **859** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorizati on	28-Feb-2023	4.3	The WP Meta SEO plugin for WordPress is vulnerable to unauthorized options update due to a missing capability check on the wpmsGGSaveInform ation function in versions up to, and including, 4.5.3. This makes it possible for authenticated attackers with subscriber-level access to update google analytics options maintained by the plugin. This vulnerability occurred as a result of the plugin relying on nonce checks as a means of access control, and that nonce being accessible to all authenticated users regardless of role. CVE ID : CVE-2023- 1022	https://plugin s.trac.wordpre ss.org/change set/2870465/ wp-meta- seo/trunk?co ntextall=1&ol d=2869205&o ld_path=%2F wp-meta- seo%2Ftrunk #file2, https://www. wordfence.co m/threat- intel/vulnerab ilities/id/702f 9d3b-5d33- 4215-ac76- 9aae3162d77 5	A-JOO-WP_M- 160323/284
Missing Authorizati on	28-Feb-2023	4.3	The WP Meta SEO plugin for WordPress is vulnerable to unauthorized plugin settings update due to a missing capability check on the saveSitemapSettings	https://plugin s.trac.wordpre ss.org/change set/2870465/ wp-meta- seo/trunk?co ntextall=1&ol d=2869205&o ld_path=%2F wp-meta-	A-JOO-WP_M- 160323/285

0-1

1-2

2-3

3-4 4-5 Page **149** of **859**

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function in versions up to, and including, 4.5.3. This makes it possible for authenticated attackers with subscriber-level access to change sitemap-related settings of the plugin. This vulnerability occurred as a result of the plugin relying on nonce checks as a means of access control, and that nonce being accessible to all authenticated users regardless of role. CVE ID : CVE-2023- 1023	seo%2Ftrunk #file2, https://www. wordfence.co m/threat- intel/vulnerab ilities/id/9d1 e498a-ddcb- 4c67-bf0d- bb45b6fe0e9d	
Missing Authorizati on	28-Feb-2023	4.3	The WP Meta SEO plugin for WordPress is vulnerable to unauthorized sitemap generation due to a missing capability check on the regenerateSitemaps function in versions up to, and including, 4.5.3. This makes it possible for authenticated attackers with subscriber-level access to generate sitemaps. This vulnerability occurred as a result	https://plugin s.trac.wordpre ss.org/change set?sfp_email= &sfph_mail=& reponame=&o ld=2870465% 40wp-meta- seo&new=287 0465%40wp- meta- seo&sfp_email =&sfph_mail=	A-JOO-WP_M- 160323/286

0-1

1-2

2-33-44-5Page 150 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the plugin relying on nonce checks as a means of access control, and that nonce being accessible to all authenticated users regardless of role. CVE ID : CVE-2023-		
			1024		
Missing Authorizati on	28-Feb-2023	4.3	The WP Meta SEO plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the listPostsCategory function in versions up to, and including, 4.5.3. This makes it possible for authenticated attackers with subscriber-level access to get post listings by category as long as those posts are published. This vulnerability occurred as a result of the plugin relying on nonce checks as a means of access control, and that nonce being accessible to all authenticated users regardless of role. CVE ID : CVE-2023- 1026	https://plugin s.trac.wordpre ss.org/change set?sfp_email= &sfph_mail=& reponame=&o ld=2870465% 40wp-meta- seo&new=287 0465%40wp- meta- seo&sfp_email =&sfph_mail=	A-J00-WP_M- 160323/287

0-1

1-2

2-3

3-4 4-5 Page **151** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorizati on	28-Feb-2023	4.3	The WP Meta SEO plugin for WordPress is vulnerable to unauthorized sitemap generation due to a missing capability check on the checkAllCategoryInSi temap function in versions up to, and including, 4.5.3. This makes it possible for authenticated attackers with subscriber-level access to obtain post categories. This vulnerability occurred as a result of the plugin relying on nonce checks as a means of access control, and that nonce being accessible to all authenticated users regardless of role. CVE ID : CVE-2023- 1027	https://plugin s.trac.wordpre ss.org/change set/2870465/ wp-meta- seo/trunk?co ntextall=1&ol d=2869205&o ld_path=%2F wp-meta- seo%2Ftrunk #file2	A-JOO-WP_M- 160323/288
Cross-Site Request Forgery (CSRF)	28-Feb-2023	4.3	The WP Meta SEO plugin for WordPress is vulnerable to Cross- Site Request Forgery in versions up to, and including, 4.5.3. This is due to missing or incorrect nonce validation on the setIgnore function. This makes it	https://plugin s.trac.wordpre ss.org/change set/2870465/ wp-meta- seo/trunk?co ntextall=1&ol d=2869205&o ld_path=%2F wp-meta- seo%2Ftrunk #file2,	A-JOO-WP_M- 160323/289

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			possible for unauthenticated attackers to update plugin options via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	https://plugin s.trac.wordpre ss.org/change set/2870465/ wp-meta- seo/tags/4.5.4 /inc/class.met aseo- admin.php				
			CVE ID : CVE-2023- 1028					
Cross-Site Request Forgery (CSRF)	24-Feb-2023	4.3	The WP Meta SEO plugin for WordPress is vulnerable to Cross- Site Request Forgery in versions up to, and including, 4.5.3. This is due to missing or incorrect nonce validation on the regenerateSitemaps function. This makes it possible for unauthenticated attackers to regenerate Sitemaps via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. CVE ID : CVE-2023-	N/A	A-JOO-WP_M- 160323/290			
Vendor: judging_management_system_project								
Product: juc	lging_manager	nent_syst	tem					
Affected Vers	sion(s): 1.0							

0-1

1-2

2-3

3-4 4-5 Page **153** of **859** 6-7 7-8

5-6

Unrestricted d Upload tile with Dangerous Type23-Feb-2023BalJudging Management System 1.0 was discovered to contain an arbitrary file upload vulnerability via the component edit, organizer.php. CVE 10 : CVE-2023- 24317N/AA-JUD-JUDC- 160323/291Vendor: kainerabiVendor: kainerabiVendor: kainerabiVendor: kainerabiA-JUD-JUDC- 160323/291Vendor: kainerabiVendor: kainerabiVendor: kainerabiVendor: kainerabiA-JUD-JUDC- 160323/291Improper Input During Web Page Generation (Cross-site Scripting)Jast State 2.1-Feb-2023The Youzify Vendor: kainerabiN/AA-KAI-YOUZ- 160323/291Vendor: kainerabiState State Scripting)Jast State StateMarket State Scripting)A-KAI-YOUZ- 160323/292Vendor: kainerabiState State StateState State StateMarket State Scripting)A-KAI-YOUZ- 160323/292Vendor: kainerabiState StateState State StateMarket State Scripting)A-KAI-YOUZ- 160323/292Vendor: kainerabiState StateState StateMarket State StateA-KAI-YOUZ- 160323/292Vendor: kainerabiState StateMissing Althetication for Critical Function in GHI be repository StateMissing StateMissing Althetication for Critical Function in GHI be repository StateMissing StateMissing Althetication for Critical Function in GHI be repository StateMissing StateMissing Althetication for StateMissing State </th <th>Weakness</th> <th>Publish Date</th> <th>CVSSv3</th> <th>Description & CVE ID</th> <th>Patch</th> <th>NCIIPC ID</th>	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation (Cross-site Scripting')Z1-Feb-2023 S.4S.4The Youzify WordPress plugin before 1.2.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.N/AA-KAI-YOUZ- 160323/292Toto (VEID: CVE-2023- 0059Missing Authentica tion for (19-Feb-2023)S.4Missing Authentica tion for Critical Function in GitHub repository kareadita/kavita prior to 0.7.0.https://github adavita/com nit/6648579 e152/92449d S816d0722b7A-KAV-KAVI- 160323/293	d Upload of File with Dangerous	23-Feb-2023	8.1	System 1.0 was discovered to contain an arbitrary file upload vulnerability via the component edit_organizer.php.	N/A	
Product: youzifyAffected Version(s): * Up to (excluding) 1.2.2Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')The Youzify WordPress plugin before 1.2.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting'A-KAI-YOUZ- 160323/292Vendor: kavitareaderVendor: kavitareaderVendor: kavitareaderVendor: kavitareaderVendor: kavitareaderMissing Authentica tion for 						
Affected Version(s): * Up to (excluding) 1.2.2Improper Neutralizat ion of Input During Web Page Generation (Cross-site Scripting')The Youzify WordPress plugin before 1.2.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.N/AA-KAI-YOUZ- 160323/292Vendor: kavitareader5.4Sembed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.N/AA-KAI-YOUZ- 160323/292Vendor: kavitareaderVendor: kavitareaderVendor: kavitareaderVendor: kavitareaderFreduct: kavitaMissing Authentica tion for Critical Function in GitHub repository kareadita/kavita prior to 0.7.0.https://github .com/kareadit a/kavita/com mit/6648b79Missing Authentica tion for Critical Function in GitHub repository kareadita/kavita prior to 0.7.0.https://github .com/kareadit a/kavita/com mit/6648b79	Vendor: kai	nelabs				
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')21-Feb-20235.4The Youzify WordPress plugin before 1.2.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.N/AA-KAI-YOUZ- 160323/292Vendor: kavitareaderVendor: kavitareaderVendor: kavitareaderVendor: kavitareaderVendor: kavitareaderVendor: kavitareaderAffected Version(s): * Up to (excluding) 0.7.0Missing Authentica tion for Critical FunctionMissing Authentication for Critical Function in GitHub repository kareadita/kavita prior to 0.7.0.https://github .com/kareadit a/kavita/com mit/6648b79 elb2P3249d S81600722b7 a3d72f259d5,	Product: yo	uzify				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')21-Feb-20235.4WordPress plugin before 1.2.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.N/AA-KAI-YOUZ- 160323/292Vendor: kave Vendor: kave Teroduct: kave ting functionVer D: CVE-2023- 0059N/AA-KAI-YOUZ- 160323/292Missing Authentica tion for Critical Function19-Feb-2023Missing AttacksMissing Authentication for Critical Function in GitHub repository kareadita/kavita prior to 0.7.0.https://github .com/kareadit a/kavita/com mit/6648679 e152192449d S816d0722b7A-KAV-KAVI- 160323/293	Affected Ver	sion(s): * Up to	(excluding	g) 1.2.2		
Product: kavitaAffected Version(s): * Up to (excluding) 0.7.0Missing Authentica tion for Critical FunctionMissing Authentication for Critical Function in GitHub repository kareadita/kavita prior to 0.7.0.https://github .com/kareadit a/kavita/com mit/6648b79 e1b2f92449d 5816d0722b7 a3d72f259d5,A-KAV-KAVI- 160323/293	Neutralizat ion of Input During Web Page Generation ('Cross-site	21-Feb-2023	5.4	WordPress plugin before 1.2.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. CVE ID : CVE-2023-	N/A	
Affected Version(s): * Up to (excluding) 0.7.0Missing Authentica tion for Critical Functionhttps://github .com/kareadit a/kavita/com mit/6648b79 e1b2f92449d 5816d0722b7 a3d72f259d5,https://github .com/kareadit a/kavita/com mit/6648b79 e1b2f92449d 5816d0722b7	Vendor: kav	vitareader				
Missing Authentica tion for Critical Function19-Feb-20233.5Missing Authentication for Critical Function in GitHub repository kareadita/kavita prior to 0.7.0.https://github .com/kareadit a/kavita/com mit/6648b79 e1b2f92449d 5816d0722b7 a3d72f259d5,A-KAV-KAVI- 160323/293	Product: ka	vita				
Missing Authentica tion for Critical Function19-Feb-20233.5Missing Authentication for Critical Function in GitHub repository kareadita/kavita prior to 0.7.0com/kareadit a/kavita/com mit/6648b79 e1b2f92449d 5816d0722b7 a3d72f259d5,A-KAV-KAVI- 160323/293	Affected Ver	sion(s): * Up to	(excluding	g) 0.7.0		
	Authentica tion for Critical	19-Feb-2023	3.5	Authentication for Critical Function in GitHub repository kareadita/kavita	.com/kareadit a/kavita/com mit/6648b79 e1b2f92449d 5816d0722b7	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1	CVSS Scoring S	Scale <u>0</u> -1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 0919	https://huntr. dev/bounties/ 3c514923- 473f-4c50- ae0d- d002a41fe70f	
Vendor: Kib					
	igato_autoresp				
Affected Ver	sion(s): * Up to	(excluding			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	4.8	The Arigato Autoresponder and Newsletter WordPress plugin before 2.1.7.2 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. CVE ID : CVE-2023-	N/A	A-KIB-ARIG- 160323/294
			0543		
Product: na	maste\!_lms				
Affected Ver	sion(s): * Up to	(excluding	g) 2.5.9.4		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	4.8	The Namaste! LMS WordPress plugin before 2.5.9.4 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html	N/A	A-KIB-NAMA- 160323/295

0-1

1-2

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			capability is disallowed (for example in multisite setup).		
			CVE ID : CVE-2023- 0548		
Product: wa	itu_quiz				
Affected Ver	sion(s): * Up to	(excluding	g) 3.3.8.2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	6.1	The Watu Quiz WordPress plugin before 3.3.8.2 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin. CVE ID : CVE-2023- 0428	N/A	A-KIB-WATU- 160323/296
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	4.8	The Watu Quiz WordPress plugin before 3.3.8.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	N/A	A-KIB-WATU- 160323/297

0-1

1-2

2-3

3-4 4-5 Page **156** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2023- 0429							
Vendor: kro	Vendor: krontech									
Product: sin	gle_connect									
Affected Ver	Affected Version(s): * Up to (excluding) 2.16.1									
Authorizati on Bypass Through User- Controlled Key	17-Feb-2023	8.8	Improper Input Validation, Authorization Bypass Through User-Controlled Key vulnerability in Kron Tech Single Connect on Windows allows Privilege Abuse. This issue affects Single Connect: 2.16. CVE ID : CVE-2023- 0882	https://docs.k rontech.com/s ingleconnect- 2-16/update- patch-rdp- proxy-idor- vulnerability	A-KRO-SING- 160323/298					
Vendor: lara	avel-admin		0002							
Product: lar										
	sion(s): 1.8.19									
Unrestricte d Upload of File with Dangerous Type	27-Feb-2023	7.2	An arbitrary file upload vulnerability in laravel-admin v1.8.19 allows attackers to execute arbitrary code via a crafted PHP file. CVE ID : CVE-2023- 24249	N/A	A-LAR-LARA- 160323/299					
Vendor: Lib										
Product: libreswan										
Affected Ver	sion(s): 4.9			Γ						
Uncontroll ed Resource Consumpti on	21-Feb-2023	6.5	Libreswan 4.9 allows remote attackers to cause a denial of service (assert failure and daemon restart) via crafted	https://github .com/libreswa n/libreswan/i ssues/954	A-LIB-LIBR- 160323/300					

 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
			TS payload with an incorrect selector length.		
			CVE ID : CVE-2023- 23009		
Vendor: Lin	uxfoundation		I		
Product: ar	go-cd				
Affected Ver	sion(s): From (i	ncluding)	2.3.0 Up to (excluding)	2.3.17	
Incorrect Authorizati on	16-Feb-2023	8.5	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All Argo CD versions starting with 2.3.0- rc1 and prior to 2.3.17, 2.4.23 2.5.11, and 2.6.2 are vulnerable to an improper authorization bug which allows users who have the ability to update at least one cluster secret to update any cluster secret. The attacker could use this access to escalate privileges (potentially controlling Kubernetes resources) or to break Argo CD functionality (by preventing connections to external clusters). A patch for this vulnerability has been released in Argo CD versions 2.6.2, 2.5.11, 2.4.23,	https://github .com/argoproj /argo- cd/commit/fb b0b99b1ac33 61b253052bd 30259fa43a52 0945, https://github .com/argoproj /argo- cd/security/a dvisories/GHS A-3jfq-742w- xg8j	A-LIN-ARGO- 160323/301

0-1

1-2

2-3 3-4 4-5 Page **158** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 2.3.17. Two workarounds are available. Either modify the RBAC configuration to completely revoke all `clusters, update` access, or use the `destinations` and `clusterResourceWhi telist` fields to apply similar restrictions as the `namespaces` and `clusterResources` fields.		
			CVE ID : CVE-2023- 23947		
Affected Ver	sion(s): From (i	ncluding)	2.4.0 Up to (excluding)	2.4.23	
Incorrect Authorizati on	16-Feb-2023	8.5	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All Argo CD versions starting with 2.3.0- rc1 and prior to 2.3.17, 2.4.23 2.5.11, and 2.6.2 are vulnerable to an improper authorization bug which allows users who have the ability to update at least one cluster secret to update any cluster secret. The attacker could use this access to escalate privileges (potentially controlling Kubernetes resources) or to	https://github .com/argoproj /argo- cd/commit/fb b0b99b1ac33 61b253052bd 30259fa43a52 0945, https://github .com/argoproj /argo- cd/security/a dvisories/GHS A-3jfq-742w- xg8j	A-LIN-ARGO- 160323/302

0-1

1-2

2-33-44-5Page 159 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			break Argo CD functionality (by preventing connections to external clusters). A patch for this vulnerability has been released in Argo CD versions 2.6.2, 2.5.11, 2.4.23, and 2.3.17. Two workarounds are available. Either modify the RBAC configuration to completely revoke all `clusters, update` access, or use the `destinations` and `clusterResourceWhi telist` fields to apply similar restrictions as the `namespaces` and `clusterResources` fields.		
			CVE ID : CVE-2023- 23947		
Affected Ver	sion(s): From (i	ncluding)	2.5.0 Up to (excluding)	2.5.11	
Incorrect Authorizati on	16-Feb-2023	8.5	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All Argo CD versions starting with 2.3.0- rc1 and prior to 2.3.17, 2.4.23 2.5.11, and 2.6.2 are vulnerable to an improper authorization bug which allows users who have the ability	https://github .com/argoproj /argo- cd/commit/fb b0b99b1ac33 61b253052bd 30259fa43a52 0945, https://github .com/argoproj /argo- cd/security/a dvisories/GHS	A-LIN-ARGO- 160323/303

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			to update at least one cluster secret to update any cluster secret. The attacker could use this access to escalate privileges (potentially controlling Kubernetes resources) or to break Argo CD functionality (by preventing connections to external clusters). A patch for this vulnerability has been released in Argo CD versions 2.6.2, 2.5.11, 2.4.23, and 2.3.17. Two workarounds are available. Either modify the RBAC configuration to completely revoke all `clusters, update` access, or use the `destinations` and `clusterResourceWhi telist` fields to apply similar restrictions as the `namespaces` and `clusterResources` fields. CVE ID : CVE-2023- 23947	A-3jfq-742w- xg8j				
Affected Ver	Affected Version(s): From (including) 2.6.0 Up to (excluding) 2.6.2							
Incorrect			Argo CD is a	https://github				
Authorizati on	16-Feb-2023	8.5	declarative, GitOps continuous delivery tool for Kubernetes.	.com/argoproj /argo- cd/commit/fb	A-LIN-ARGO- 160323/304			

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			All Argo CD versions	b0b99b1ac33	
			starting with 2.3.0-	61b253052bd	
			rc1 and prior to	30259fa43a52	
			2.3.17, 2.4.23 2.5.11,	0945,	
			and 2.6.2 are	https://github	
			vulnerable to an	.com/argoproj	
			improper	/argo-	
			authorization bug	cd/security/a	
			which allows users	dvisories/GHS	
			who have the ability	A-3jfq-742w-	
			to update at least	xg8j	
			one cluster secret to		
			update any cluster		
			secret. The attacker		
			could use this access		
			to escalate privileges		
			(potentially		
			controlling		
			Kubernetes		
			resources) or to		
			break Argo CD		
			functionality (by		
			preventing		
			connections to		
			external clusters). A		
			patch for this		
			vulnerability has		
			been released in		
			Argo CD versions		
			2.6.2, 2.5.11, 2.4.23,		
			and 2.3.17. Two		
			workarounds are		
			available. Either		
			modify the RBAC		
			configuration to		
			completely revoke all		
			`clusters, update`		
			access, or use the `destinations` and		
			`clusterResourceWhi		
			telist` fields to apply		
			similar restrictions		
			as the `namespaces`		
			and		
			anu		

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			`clusterResources` fields. CVE ID : CVE-2023- 23947						
Product: co	Product: containerd								
Affected Ver	sion(s): * Up to	(excluding	g) 1.5.18						
Incorrect Authorizati on	16-Feb-2023	7.8	containerd is an open source container runtime. A bug was found in containerd prior to versions 1.6.18 and 1.5.18 where supplementary groups are not set up properly inside a container. If an attacker has direct access to a container and manipulates their supplementary group access, they may be able to use supplementary group access to bypass primary group restrictions in some cases, potentially gaining access to sensitive information or gaining the ability to execute code in that container. Downstream applications that use the containerd client library may be affected as well. This bug has been fixed in containerd v1.6.18 and v.1.5.18. Users should update to	https://github .com/containe rd/containerd /commit/133f 6bb6cd827ce 35a5fb279c1e ad12b9d2146 0a, https://github .com/containerd /security/advi sories/GHSA- hmfx-3pcx- 653p	A-LIN-CONT- 160323/305				

0-1

1-2

2-33-44-5Page 163 of 859

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these versions and recreate containers to resolve this issue. Users who rely on a downstream application that uses containerd's client library should check that application for a separate advisory and instructions. As a workaround, ensure that the `"USER \$USERNAME"` Dockerfile instruction is not used. Instead, set the container entrypoint to a value similar to `ENTRYPOINT ["su", "-", "user"]` to allow `su` to properly set up supplementary groups. CVE ID : CVE-2023- 25173		
Allocation of Resources Without Limits or Throttling	16-Feb-2023	5.5	containerd is an open source container runtime. Before versions 1.6.18 and 1.5.18, when importing an OCI image, there was no limit on the number of bytes read for certain files. A maliciously crafted image with a large file where a limit was not applied could cause a denial of service. This bug has	https://github .com/containe rd/containerd /commit/0c3 14901076a74 a7b797a545d 2f462285fdbb 8c4, https://github .com/containe rd/containerd /security/advi sories/GHSA- 259w-8hf6- 59c2	A-LIN-CONT- 160323/306

0-1

1-2

2-3

3-4 4-5 Page **164** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been fixed in containerd 1.6.18 and 1.5.18. Users should update to these versions to resolve the issue. As a workaround, ensure that only trusted images are used and that only trusted users have permissions to import images. CVE ID : CVE-2023- 25153		
Affected Ver	sion(s): From (i	ncluding)	1.6.0 Up to (excluding)	1.6.18	
Incorrect Authorizati on	16-Feb-2023	7.8	containerd is an open source container runtime. A bug was found in containerd prior to versions 1.6.18 and 1.5.18 where supplementary groups are not set up properly inside a container. If an attacker has direct access to a container and manipulates their supplementary group access, they may be able to use supplementary group access to bypass primary group restrictions in some cases, potentially gaining access to sensitive information or gaining the ability to execute code in that	https://github .com/containe rd/containerd /commit/133f 6bb6cd827ce 35a5fb279c1e ad12b9d2146 0a, https://github .com/containe rd/containerd /security/advi sories/GHSA- hmfx-3pcx- 653p	A-LIN-CONT- 160323/307

0-1

1-2

2-3

3-4 4-5 Page **165** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			container. Downstream applications that use the containerd client library may be affected as well. This bug has been fixed in containerd v1.6.18 and v.1.5.18. Users should update to these versions and recreate containers to resolve this issue. Users who rely on a downstream application that uses containerd's client library should check that application for a separate advisory and instructions. As a workaround, ensure that the `"USER \$USERNAME"` Dockerfile instruction is not used. Instead, set the container entrypoint to a value similar to `ENTRYPOINT ["su", "-", "user"]` to allow `su` to properly set up supplementary groups. CVE ID : CVE-2023- 25173		
Allocation of Resources Without Limits or Throttling	16-Feb-2023	5.5	containerd is an open source container runtime. Before versions 1.6.18 and 1.5.18, when importing an	https://github .com/containe rd/containerd /commit/0c3 14901076a74 a7b797a545d	A-LIN-CONT- 160323/308

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OCI image, there was no limit on the number of bytes read for certain files. A maliciously crafted image with a large file where a limit was not applied could cause a denial of service. This bug has been fixed in containerd 1.6.18 and 1.5.18. Users should update to these versions to resolve the issue. As a workaround, ensure that only trusted images are used and that only trusted users have permissions to import images. CVE ID : CVE-2023- 25153	2f462285fdbb 8c4, https://github .com/containe rd/containerd /security/advi sories/GHSA- 259w-8hf6- 59c2	
Vendor: lite	-web-server_p	roject			
Product: lite	e-web-server				
Affected Ver	sion(s): -				
Uncontroll ed Resource Consumpti on	25-Feb-2023	7.5	All versions of the package lite-web- server are vulnerable to Denial of Service (DoS) when an attacker sends an HTTP request and includes control characters that the decodeURI() function is unable to parse. CVE ID : CVE-2023- 26104	N/A	A-LIT-LITE- 160323/309

0-1

1-2

2-33-44-5Page 167 of 859

6-7

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Vendor: loa	n_comparison_	project	L	L	L				
Product: loa	Product: loan_comparison								
Affected Version(s): * Up to (excluding) 1.5.3									
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	6.1	The Loan Comparison WordPress plugin before 1.5.3 does not validate and escape some of its query parameters before outputting them back in a page/post via an embedded shortcode, which could allow an attacker to inject javascript into into the site via a crafted URL. CVE ID : CVE-2023- 0442	N/A	A-LOA-LOAN- 160323/310				
Vendor: luc	kyframe			L					
Product: luc	kyframeweb								
Affected Vers	sion(s): 3.5								
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	9.8	LuckyframeWEB v3.5 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /system/UserMappe r.xml. CVE ID : CVE-2023- 24219	https://github .com/seagull1 985/LuckyFra meWeb/issue s/24	A-LUC-LUCK- 160323/311				
Improper Neutralizat ion of Special Elements used in an	17-Feb-2023	9.8	LuckyframeWEB v3.5 was discovered to contain a SQL injection vulnerability via the dataScope parameter	https://github .com/seagull1 985/LuckyFra meWeb/issue s/22	A-LUC-LUCK- 160323/312				
CVSS Scoring S	icale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	3 <u>8-9</u> <u>9-10</u>				

Page 168 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			at /system/RoleMappe r.xml. CVE ID : CVE-2023- 24220		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL	17-Feb-2023	9.8	LuckyframeWEB v3.5 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /system/DeptMappe r.xml. CVE ID : CVE-2023-	https://github .com/seagull1 985/LuckyFra meWeb/issue s/23	A-LUC-LUCK- 160323/313
Injection')			24221		
Vendor: ma	-				
Product: me					
Affected Ver	sion(s): * Up to	(excluding		1	
Cross-Site Request Forgery (CSRF)	23-Feb-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in MainWP Matomo Extension <= 4.0.4 versions. CVE ID : CVE-2023- 23659	N/A	A-MAI-MOTO- 160323/314
Vendor: Ma	ntisbt				
Product: ma	antisbt				
Affected Ver	sion(s): * Up to	(excluding	g) 2.25.6		
N/A	23-Feb-2023	4.3	Mantis Bug Tracker (MantisBT) is an open source issue tracker. In versions prior to 2.25.6, due to insufficient access-level checks, any logged-in user allowed to perform Group Actions can	https://www. mantisbt.org/ bugs/view.ph p?id=31086	A-MAN-MANT- 160323/315

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
			access to the _Summary_field of private Issues (i.e. having Private view status, or belonging to a private Project) via a crafted `bug_arr[]` parameter in *bug_actiongroup_ex t.php*. This issue is fixed in version 2.25.6. There are no workarounds.		
Vendor: ma	rkdown-electr	on proje	22476		
	arkdown-elect				
Affected Vers	sion(s): -				
Improper Control of Generation of Code ('Code Injection')	24-Feb-2023	7.8	A vulnerability was found in JP1016 Markdown-Electron and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to code injection. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are	N/A	A-MAR-MARK- 160323/316

0-1

1-2

2-33-44-5Page 170 of 859

6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			available. VDB- 221738 is the identifier assigned to this vulnerability.		
			CVE ID : CVE-2023- 1005		
Vendor: ma	rktext				1
Product: ma	ırktext				
Affected Vers	sion(s): * Up to	(including	g) 0.17.1	-	-
Improper Control of Generation of Code ('Code Injection')	24-Feb-2023	7.8	A vulnerability has been found in MarkText up to 0.17.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the component WSH JScript Handler. The manipulation leads to code injection. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-221737 was assigned to this vulnerability. CVE ID : CVE-2023-	N/A	A-MAR-MARK- 160323/317
Vendor: ma	ttermost		1004		
Product: ma					
Affected Vers	sion(s): * Up to	(including	g) 7.1.4		
Missing Authorizati on	27-Feb-2023	6.5	A missing permissions check in the /plugins/playbooks/ api/v0/runs API in	https://matte rmost.com/se curity- updates/	A-MAT-MATT- 160323/318
CVSS Scoring S	icale 0-1	1-2 2	<mark>-3 3-4 4-5 5</mark> Page 171 of 859	-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mattermost allows an attacker to list and view playbooks belonging to a team they are not a member of.		
			CVE ID : CVE-2023- 27263		
Missing Authorizati on	27-Feb-2023	6.5	A missing permissions check in Mattermost Playbooks in Mattermost allows an attacker to modify a playbook via the /plugins/playbooks/[p laybookID] API.	https://matte rmost.com/se curity- updates/	A-MAT-MATT- 160323/319
			CVE ID : CVE-2023- 27264		
Affected Ver	sion(s): 7.4.0			I	1
Missing Authorizati on	27-Feb-2023	6.5	A missing permissions check in the /plugins/playbooks/ api/v0/runs API in Mattermost allows an attacker to list and view playbooks belonging to a team they are not a member of.	https://matte rmost.com/se curity- updates/	A-MAT-MATT- 160323/320
			CVE ID : CVE-2023- 27263		
Missing Authorizati on	27-Feb-2023	6.5	A missing permissions check in Mattermost Playbooks in Mattermost allows an attacker to modify a playbook via the /plugins/playbooks/	https://matte rmost.com/se curity- updates/	A-MAT-MATT- 160323/321

0-1

1-2

2-3

8-9

9-10

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			api/v0/playbooks/[p laybookID] API.		
			CVE ID : CVE-2023- 27264		
Affected Ver	sion(s): 7.5.0				
Missing Authorizati on	27-Feb-2023	6.5	A missing permissions check in the /plugins/playbooks/ api/v0/runs API in Mattermost allows an attacker to list and view playbooks belonging to a team they are not a member of.	https://matte rmost.com/se curity- updates/	A-MAT-MATT- 160323/322
			CVE ID : CVE-2023- 27263		
Missing Authorizati on	27-Feb-2023	6.5	A missing permissions check in Mattermost Playbooks in Mattermost allows an attacker to modify a playbook via the /plugins/playbooks/ api/v0/playbooks/[p laybookID] API. CVE ID : CVE-2023- 27264	https://matte rmost.com/se curity- updates/	A-MAT-MATT- 160323/323
Affected Ver	sion(s): 7.5.1				
Missing Authorizati on	27-Feb-2023	6.5	A missing permissions check in the /plugins/playbooks/ api/v0/runs API in Mattermost allows an attacker to list and view playbooks belonging to a team	https://matte rmost.com/se curity- updates/	A-MAT-MATT- 160323/324

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			they are not a member of. CVE ID : CVE-2023-		
Missing Authorizati on	27-Feb-2023	6.5	27263 A missing permissions check in Mattermost Playbooks in Mattermost allows an attacker to modify a playbook via the /plugins/playbooks/ api/v0/playbooks/ [p laybookID] API. CVE ID : CVE-2023- 27264	https://matte rmost.com/se curity- updates/	A-MAT-MATT- 160323/325
Product: ma	attermost_serv	er			
Affected Ver	sion(s): From (i	ncluding)	5.12.0 Up to (excluding) 7.7.0	
Exposure of Resource to Wrong Sphere	27-Feb-2023	2.7	Mattermost fails to honor the ShowEmailAddress setting when constructing a response to the "Regenerate Invite Id" API endpoint, allowing an attacker with team admin privileges to learn the team owner's email address in the response. CVE ID : CVE-2023-	https://matte rmost.com/se curity- updates/	A-MAT-MATT- 160323/326
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	27-Feb-2023	2.7	27265 Mattermost fails to honor the ShowEmailAddress setting when constructing a response to the /api/v4/users/me/t	https://matte rmost.com/se curity- updates/	A-MAT-MATT- 160323/327

0-1

1-2

2-3 3-4 4-5 Page **174** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description	& CVE ID		Patch		NCIIF	CID
			eams API en allowing an with team a privileges to the team ow email addre response.	attacker dmin o learn vner's ss in the					
			CVE ID : CV 27266	E-2023-					
	dia_library_ass	-	roject						
	edia_library_as		a) 3.06						
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	7.2	The Media I Assistant W plugin befor does not pro sanitise and parameter b using it in a statement, l a SQL inject exploitable privilege us as admin. CVE ID : CV 0279	ordPress re 3.06 operly escape a before SQL eading to ion by high ers such	N/A			A-MED-N 160323/	
Vendor: me	dical_certificat	te_genera	tor_app_pro	ject	I				
Product: me	edical_certifica	te_gener	ator_app						
Affected Vers	sion(s): 1.0								
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	24-Feb-2023	5.4	A vulnerabil found in SourceCode Medical Cer Generator A has been cla problematic affects an un part of the component Record Han manipulatio	ster tificate app 1.0. It assified as c. This nknown New dler. The	N/A			A-MED-M 160323/	
CVSS Scoring S	icale 0-1	1-2 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
			argument Firstname/Middlena me/Lastname/Suffix /Nationality/Doctor Fullname/Doctor Suffix with the input "> <script>prompt(1) </script> leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB- 221739.		
			CVE ID : CVE-2023- 1006		
Vendor: Mic					
Product: mi	croweber				
Affected Ver	sion(s): * Up to	(including	g) 1.3.2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	28-Feb-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microw eber prior to 1.3.3. CVE ID : CVE-2023- 1081	https://github .com/microwe ber/microweb er/commit/29 d418461d840 7688f2720e7 b4be915e03fc 16c1, https://huntr. dev/bounties/ cf59deed- 9d43-4552- acfd- 43f38f3aabba	A-MIC-MICR- 160323/330
Vendor: mii					
Product: mi Affected Ver 17t17-52-43	sion(s): From (i	ncluding)	2020-04-10t03-34-42z	Up to (excluding	y) 2023-02-
N/A	21-Feb-2023	8.8	Minio is a Multi- Cloud Object Storage framework. Affected	https://github .com/minio/ minio/securit	A-MIN-MINI- 160323/331
		1 2		6 67 7	
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 176 of 859	-6 6-7 7-8	8 8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions do not correctly honor a `Deny` policy on ByPassGoverance. Ideally, minio should return "Access Denied" to all users attempting to DELETE a versionId with the special header `X-Amz- Bypass-Governance- Retention: true`. However, this was not honored instead the request will be honored and an object under governance would be incorrectly deleted. All users are advised to upgrade. There are no known workarounds for this issue. CVE ID : CVE-2023- 25812	y/advisories/ GHSA-c8fc- mjj8-fc63, https://github .com/minio/ minio/commit /a7188bc9d0f 0a5ae05aaf1b 8126bcd3cb3f dc485, https://github .com/minio/ minio/pull/16 635	
Vendor: mis	sskey				
Product: mi					
Affected Ver	sion(s): * Up to	(excluding			
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	22-Feb-2023	9.8	Misskey is an open source, decentralized social media platform. In versions prior to 13.3.3 SQL injection is possible due to insufficient parameter validation in the note search API by tag (notes/search-by- tag). This has been	https://github .com/misskey - dev/misskey/ security/advis ories/GHSA- cgwp-vmr4- wx4q, https://github .com/misskey - dev/misskey/	A-MIS-MISS- 160323/332

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in version 13.3.3. Users are advised to upgrade. Users unable to upgrade should block access to the `api/notes/search- by-tag` endpoint. CVE ID : CVE-2023-	commit/ee74 df68233adcd5 b167258c621 565f97c3b23 06	
			24812		
	sion(s): * Up to	Cexcluuin	Misskey is an open		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	22-Feb-2023	6.1	source, decentralized social media platform. Due to insufficient validation of the redirect URL during `miauth` authentication in Misskey, arbitrary JavaScript can be executed when a user allows the link. All versions below 13.3.1 (including 12.x) are affected. This has been fixed in version 13.3.1. Users are advised to upgrade. Users unable to upgrade should not allow authentication of untrusted apps. CVE ID : CVE-2023- 24810	https://github .com/misskey - dev/misskey/ security/advis ories/GHSA- cc6r-chgr- 8r5m	A-MIS-MISS- 160323/333
Affected Ver	sion(s): * Up to	(excluding	g) 13.3.2		
Improper Neutralizat ion of Input	22-Feb-2023	6.1	Misskey is an open source, decentralized social media platform. In versions	https://github .com/misskey - dev/misskey/	A-MIS-MISS- 160323/334

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			prior to 13.3.2 the URL preview function is subject to a cross site scripting vulnerability due to insufficient URL validation. Arbitrary JavaScript is executed when a malicious URL is loaded in the `View in Player` or `View in Window` preview. This has been fixed in version 13.3.2. Users are advised to upgrade. Users unable to upgrade should avoid usage of the `View in Player` or `View in Window` functions.	commit/38f9d 1e76428bea4 7c5944c440e ab25428c7d9 9e, https://github .com/misskey - dev/misskey/ security/advis ories/GHSA- vc39-c453- 67g3	
			CVE ID : CVE-2023- 24811		
Affected Ver	sion(s): * Up to	(excluding	g) 13.5.0		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	22-Feb-2023	6.1	Misskey is an open source, decentralized social media platform. In versions prior to 13.5.0 the link to the instance to the sender that appears when viewing a user or note received through ActivityPub is not properly validated, so by inserting a URL with a javascript scheme an attacker may execute JavaScript code in the context of	https://github .com/misskey - dev/misskey/ security/advis ories/GHSA- pfp5-r48x- fg25	A-MIS-MISS- 160323/335

0-1

1-2

2-33-44-5Page 179 of 859

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the recipient. This issue has been fixed in version 13.5.0. Users are advised to upgrade. Users unable to upgrade should not "view on remote" for untrusted instances.		
			CVE ID : CVE-2023- 25154		
Vendor: mo	doboa			<u> </u>	
Product: ins	staller				
Affected Ver	sion(s): * Up to	(excluding	g) 2.0.4		
Improper Restriction of Excessive Authentica tion Attempts	16-Feb-2023	7.5	Improper Restriction of Excessive Authentication Attempts in GitHub repository modoboa/modoboa- installer prior to 2.0.4. CVE ID : CVE-2023- 0860	https://huntr. dev/bounties/ 64f3ab93- 1357-4468- 8ff4- 52bbcec18cca, https://github .com/modobo a/modoboa- installer/com mit/63d92b7 3f3da6971ae4 e13d033d625 773ac91085	A-MOD-INST- 160323/336
Product: mo					
Affected Ver	sion(s): * Up to	(excluding	g) 2.0.5		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	22-Feb-2023	4.8	Cross-site Scripting (XSS) - Reflected in GitHub repository modoboa/modoboa prior to 2.0.5. CVE ID : CVE-2023- 0949	https://github .com/modobo a/modoboa/c ommit/aa74e 9a4a870162e ea169e0a6a2e ab841f8811b 7, https://huntr. dev/bounties/ ef87be4e-	A-MOD-MODO- 160323/337

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				493b-4ee9- 9738- 44c55b8acc19	
Vendor: mo	d_gnutls_proje	ct			
Product: mo	od_gnutls				
Affected Ver	sion(s): From (i	ncluding)	0.9.0 Up to (including)	1.2.0	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	23-Feb-2023	7.5	Mod_gnutls is a TLS module for Apache HTTPD based on GnuTLS. Versions from 0.9.0 to 0.12.0 (including) did not properly fail blocking read operations on TLS connections when the transport hit timeouts. Instead it entered an endless loop retrying the read operation, consuming CPU resources. This could be exploited for denial of service attacks. If trace level logging was enabled, it would also produce an excessive amount of log output during the loop, consuming disk space. The problem has been fixed in commit d7eec4e598158ab6a 98bf505354e84352f 9715ec, please update to version 0.12.1. There are no workarounds, users who cannot update should apply the	https://github .com/airtower - luna/mod_gnu tls/commit/d 7eec4e59815 8ab6a98bf505 354e84352f9 715ec, https://github .com/airtower - luna/mod_gnu tls/security/a dvisories/GHS A-6cfv-fvgm- 7pc8, https://bugs.d ebian.org/cgi- bin/bugreport .cgi?bug=9427 37#25	A-MOD-MOD 160323/338

0-1

1-2

2-33-44-5Page 181 of 859

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			errno fix detailed in the security advisory.		
			CVE ID : CVE-2023- 25824		
Vendor: Mo	no-project				
Product: mo	ono				
Affected Ver	sion(s): 5.18.0.2	240\\+dfs	g-3		
N/A	22-Feb-2023	8.8	The mono package before 6.8.0.105+dfsg-3.3 for Debian allows arbitrary code execution because the application/x- ms-dos-executable MIME type is associated with an un-sandboxed Mono CLR interpreter. CVE ID : CVE-2023-	N/A	A-MON-MONO- 160323/339
Affected Ver	sion(s): 6.8.0.10)5\\+dfsg	26314		
N/A	22-Feb-2023	8.8	The mono package before 6.8.0.105+dfsg-3.3 for Debian allows arbitrary code execution because the application/x- ms-dos-executable MIME type is associated with an un-sandboxed Mono CLR interpreter. CVE ID : CVE-2023- 26314	N/A	A-MON-MONO- 160323/340
Vendor: Mo	odle				
Product: mo	oodle				
Affected Ver	sion(s): 4.1.0				
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5	5-6 6-7 7-8	8 8-9 9-10
			Page 182 of 859		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Feb-2023	8.2	The vulnerability was found Moodle which exists due to insufficient limitations on the "start page" preference. A remote attacker can set that preference for another user. The vulnerability allows a remote attacker to gain unauthorized access to otherwise restricted functionality. CVE ID : CVE-2023- 23923	https://moodl e.org/mod/fo rum/discuss.p hp?d=443274 #p1782023, http://git.moo dle.org/gw?p= moodle.git&a= search&h=HE AD&st=commi t&s=MDL- 76862	A-M00-M00D- 160323/341
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	6.1	The vulnerability was found Moodle which exists due to insufficient sanitization of user- supplied data in some returnurl parameters. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks. CVE ID : CVE-2023- 23921	http://git.moo dle.org/gw?p= moodle.git&a= search&h=HE AD&st=commi t&s=MDL- 76810, https://moodl e.org/mod/fo rum/discuss.p hp?d=443272 #p1782021	A-M00-M00D- 160323/342

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	6.1	The vulnerability was found Moodle which exists due to insufficient sanitization of user- supplied data in blog search. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks. CVE ID : CVE-2023- 23922	https://moodl e.org/mod/fo rum/discuss.p hp?d=443273 #p1782022, http://git.moo dle.org/gw?p= moodle.git&a= search&h=HE AD&st=commi t&s=MDL- 76861	A-M00-M00D- 160323/343
N/A	17-Feb-2023	8.2	3.11.0 Up to (excluding The vulnerability was found Moodle which exists due to insufficient limitations on the "start page" preference. A remote attacker can set that preference for another user. The vulnerability allows a remote attacker to gain unauthorized access to otherwise restricted functionality. CVE ID : CVE-2023- 23923	https://moodl e.org/mod/fo rum/discuss.p hp?d=443274 #p1782023, http://git.moo dle.org/gw?p= moodle.git&a= search&h=HE AD&st=commi t&s=MDL- 76862	A-MOO-MOOD- 160323/344

0-1

1-2

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	6.1	The vulnerability was found Moodle which exists due to insufficient sanitization of user- supplied data in some returnurl parameters. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks. CVE ID : CVE-2023- 23921	http://git.moo dle.org/gw?p= moodle.git&a= search&h=HE AD&st=commi t&s=MDL- 76810, https://moodl e.org/mod/fo rum/discuss.p hp?d=443272 #p1782021	A-M00-M00D- 160323/345
Affected Ver	sion(s): From (i	ncluding)	3.9.0 Up to (excluding)	3.9.19	
N/A	17-Feb-2023	8.2	The vulnerability was found Moodle which exists due to insufficient limitations on the "start page" preference. A remote attacker can set that preference for another user. The vulnerability allows a remote attacker to gain unauthorized access to otherwise restricted functionality.	https://moodl e.org/mod/fo rum/discuss.p hp?d=443274 #p1782023, http://git.moo dle.org/gw?p= moodle.git&a= search&h=HE AD&st=commi t&s=MDL- 76862	A-MOO-MOOD- 160323/346

0-1

1-2

2-33-44-5Page 185 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23923		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	6.1	The vulnerability was found Moodle which exists due to insufficient sanitization of user- supplied data in some returnurl parameters. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks. CVE ID : CVE-2023- 23921	http://git.moo dle.org/gw?p= moodle.git&a= search&h=HE AD&st=commi t&s=MDL- 76810, https://moodl e.org/mod/fo rum/discuss.p hp?d=443272 #p1782021	A-M00-M00D- 160323/347
Affected Ver	<mark>sion(s): From (</mark> i	ncluding)	4.0.0 Up to (excluding)	4.0.6	L
N/A	17-Feb-2023	8.2	The vulnerability was found Moodle which exists due to insufficient limitations on the "start page" preference. A remote attacker can set that preference for another user. The vulnerability allows a remote attacker to gain unauthorized access to otherwise	https://moodl e.org/mod/fo rum/discuss.p hp?d=443274 #p1782023, http://git.moo dle.org/gw?p= moodle.git&a= search&h=HE AD&st=commi t&s=MDL- 76862	A-MOO-MOOD- 160323/348

0-1

1-2

2-33-44-5Page 186 of 859

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restricted functionality. CVE ID : CVE-2023- 23923		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	6.1	The vulnerability was found Moodle which exists due to insufficient sanitization of user- supplied data in some returnurl parameters. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks. CVE ID : CVE-2023- 23921	http://git.moo dle.org/gw?p= moodle.git&a= search&h=HE AD&st=commi t&s=MDL- 76810, https://moodl e.org/mod/fo rum/discuss.p hp?d=443272 #p1782021	A-M00-M00D- 160323/349
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	6.1	The vulnerability was found Moodle which exists due to insufficient sanitization of user- supplied data in blog search. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website.	https://moodl e.org/mod/fo rum/discuss.p hp?d=443273 #p1782022, http://git.moo dle.org/gw?p= moodle.git&a= search&h=HE AD&st=commi t&s=MDL- 76861	A-M00-M00D- 160323/350

0-1

1-2

2-3

3-4 4-5 Page **187** of **859** 5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks. CVE ID : CVE-2023- 23922		
Vendor: mo	osikay_e-comr	nerce_sys	stem_project		
Product: mo	oosikay_e-com	merce_sy	stem		
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	24-Feb-2023	8.8	A vulnerability was found in SourceCodester Moosikay E- Commerce System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /Moosikay/order.ph p of the component POST Parameter Handler. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221732. CVE ID : CVE-2023-	N/A	A-M00-M00S- 160323/351
Vendor: mu	sic_gallery_site	e_project	0997		
Product: m	usic_gallery_sit	e			
Affected Ver	sion(s): 1.0				
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10
			Page 188 of 859		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Music Gallery Site 1.0. This affects an unknown part of the file music_list.php of the component GET Request Handler. The manipulation of the argument cid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB- 221553 was assigned to this vulnerability. CVE ID : CVE-2023- 0938	N/A	A-MUS-MUSI- 160323/352
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	22-Feb-2023	9.8	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been classified as critical. This affects an unknown part of the file view_music_details.p hp of the component GET Request Handler. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely.	N/A	A-MUS-MUSI- 160323/353

0-1

1-2

2-3 3-4 4-5 Page **189** of **859** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB- 221631.		
			CVE ID : CVE-2023- 0961		
Improper Access Control	22-Feb-2023	9.8	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been rated as critical. This issue affects some unknown processing of the file Users.php of the component POST Request Handler. The manipulation leads to improper access controls. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB- 221633 was assigned to this vulnerability. CVE ID : CVE-2023- 0963	N/A	A-MUS-MUSI- 160323/354
Improper Neutralizat ion of Special Elements used in an SQL Command	27-Feb-2023	9.8	A vulnerability was found in SourceCodester Music Gallery Site 1.0 and classified as critical. This issue affects some unknown processing	N/A	A-MUS-MUSI- 160323/355

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			of the file view_category.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB- 221819. CVE ID : CVE-2023- 1053		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	9.8	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/?page=user/ manage. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB- 221820. CVE ID : CVE-2023-	N/A	A-MUS-MUSI- 160323/356
Improper Neutralizat ion of Special Elements used in an SQL Command	22-Feb-2023	8.8	1054 A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been declared as critical. This vulnerability affects unknown code of the file	N/A	A-MUS-MUSI- 160323/357

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			Master.php of the component GET Request Handler. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221632. CVE ID : CVE-2023- 0962		
Vendor: mu	yucms				
Product: m	uyucms				
Affected Ver	sion(s): 2.2				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Feb-2023	8.8	A vulnerability was found in MuYuCMS 2.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /editor/index.php. The manipulation of the argument file_path leads to relative path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier	N/A	A-MUY-MUYU- 160323/358

0-1

1-2

2-33-44-5Page 192 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability is VDB-221803.		
			CVE ID : CVE-2023- 1044		
Server- Side Request Forgery (SSRF)	26-Feb-2023	8.8	A vulnerability classified as critical has been found in MuYuCMS 2.2. This affects an unknown part of the file /admin.php/update/ getFile.html. The manipulation of the argument url leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221805 was assigned to this vulnerability. CVE ID : CVE-2023-	N/A	A-MUY-MUYU- 160323/359
			1046		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Feb-2023	8.1	A vulnerability was found in MuYuCMS 2.2. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin.php/accesso ry/filesdel.html. The manipulation of the argument filedelur leads to relative path traversal. The attack may be launched remotely. The exploit	N/A	A-MUY-MUYU- 160323/360

0-1

1-2

2-3

3-4 4-5 Page 193 of 859

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. The identifier of this vulnerability is VDB- 221804.		
			CVE ID : CVE-2023- 1045		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Feb-2023	6.5	A vulnerability, which was classified as problematic, has been found in MuYuCMS 2.2. This issue affects some unknown processing of the file index.php. The manipulation of the argument file_path leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB- 221735. CVE ID : CVE-2023- 1002	N/A	A-MUY-MUYU- 160323/361
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Feb-2023	4.3	A vulnerability was found in MuYuCMS 2.2. It has been classified as problematic. Affected is an unknown function of the file /editor/index.php. The manipulation of the argument dir_path leads to	N/A	A-MUY-MUYU- 160323/362

0-1

1-2

2-3

7-8

6-7

5-6

-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			relative path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-221802 is the identifier assigned to this vulnerability. CVE ID : CVE-2023-		
			1043		
	-automation				
Product: lib					
Affected Ver	sion(s): 2.3.2			1	
Missing Release of Memory after Effective Lifetime	24-Feb-2023	5.5	An issue was discovered in lib60870 v2.3.2. There is a memory leak in lib60870/lib60870- C/examples/multi_cl ient_server/multi_cli ent_server.c. CVE ID : CVE-2023-	N/A	A-MZLIB6- 160323/363
			23205		
Vendor: Neo					
	vesome_proced				
Affected Ver	sion(s): * Up to	(excluding		[
Improper Restriction of XML External Entity Reference	16-Feb-2023	8.1	APOC (Awesome Procedures on Cypher) is an add-on library for Neo4j. An XML External Entity (XXE) vulnerability found in the apoc.import.graphml procedure of APOC core plugin prior to version 5.5.0 in	https://github .com/neo4j/a poc/pull/310, https://github .com/neo4j/a poc/security/ advisories/GH SA-6wxg- wh7f-rqpr	A-NEO-AWES- 160323/364
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	³ 8-9 9-10

Page 195 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Neo4j graph		
			database. XML		
			External Entity (XXE)		
			injection occurs		
			when the XML parser		
			allows external		
			entities to be		
			resolved. The XML		
			parser used by the		
			apoc.import.graphml		
			procedure was not		
			configured in a		
			secure way and		
			therefore allowed		
			this. External entities		
			can be used to read		
			local files, send HTTP		
			requests, and		
			perform denial-of-		
			service attacks on		
			the application.		
			Abusing the XXE		
			vulnerability enabled		
			assessors to read		
			local files remotely.		
			Although with the		
			level of privileges		
			assessors had this		
			was limited to one-		
			line files. With the		
			ability to write to the		
			database, any file		
			could have been		
			read. Additionally,		
			assessors noted, with		
			local testing, the		
			server could be		
			crashed by passing		
			in improperly		
			formatted XML. The		
			minimum version		
			containing a patch		
			for this vulnerability		
			is 5.5.0. Those who		

0-1

1-2

2-3

3-4 4-5 Page **196** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cannot upgrade the library can control the allowlist of the procedures that can be used in your system.		
			CVE ID : CVE-2023- 23926		
Vendor: nethack					
Product: nethack					
Affected Version(s): From (including) 3.6.2 Up to (excluding) 3.6.7					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Feb-2023	5.5	NetHack is a single player dungeon exploration game. Starting with version 3.6.2 and prior to version 3.6.7, illegal input to the "C" (call) command can cause a buffer overflow and crash the NetHack process. This vulnerability may be a security issue for systems that have NetHack installed suid/sgid and for shared systems. For all systems, it may result in a process crash. This issue is resolved in NetHack 3.6.7. There are no known workarounds. CVE ID : CVE-2023- 24809	https://github .com/NetHack /NetHack/sec urity/advisori es/GHSA- 2cqv-5w4v- mgch, https://netha ck.org/securit y/CVE-2023- 24809.html	A-NET-NETH- 160323/365
Vendor: netmodule Product: netmodule router software					
Product: netmodule_router_software Affected Version(s): From (including) 4.3.0.0 Up to (excluding) 4.3.0.119					
Anected version(s): From (including) 4.3.0.0 op to (excluding) 4.3.0.119					

0-1

1-2

2-3

3-4 4-5 Page **197** of **859** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	NetModule NSRW web administration interface executes an OS command constructed with unsanitized user input. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. This issue affects NSRW: from 4.3.0.0 before 4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103. CVE ID : CVE-2023- 0861	N/A	A-NET-NETM- 160323/366
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	8.8	The NetModule NSRW web administration interface is vulnerable to path traversals, which could lead to arbitrary file uploads and deletion. By uploading malicious files to the web root directory, authenticated users could gain remote command execution with elevated privileges. This issue affects NSRW: from 4.3.0.0 before	https://share. netmodule.co m/public/syst em- software/4.7/ 4.7.0.103/NRS W-RN- 4.7.0.103.pdf	A-NET-NETM- 160323/367

0-1

1-2

2-33-44-5Page 198 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103. CVE ID : CVE-2023- 0862		
Affected Ver	sion(s): From (i	ncluding)	4.4.0.0 Up to (excluding	g) 4.4.0.118	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	NetModule NSRW web administration interface executes an OS command constructed with unsanitized user input. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. This issue affects NSRW: from 4.3.0.0 before 4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103. CVE ID : CVE-2023- 0861	N/A	A-NET-NETM- 160323/368
Improper Limitation of a Pathname to a Restricted Directory	16-Feb-2023	8.8	The NetModule NSRW web administration interface is vulnerable to path traversals, which could lead to arbitrary file uploads	https://share. netmodule.co m/public/syst em- software/4.7/ 4.7.0.103/NRS W-RN- 4.7.0.103.pdf	A-NET-NETM- 160323/369

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')	sion(s): From (i	ncluding)	and deletion. By uploading malicious files to the web root directory, authenticated users could gain remote command execution with elevated privileges. This issue affects NSRW: from 4.3.0.0 before 4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103. CVE ID : CVE-2023- 0862 4.6.0.0 Up to (excluding	J) 4.6.0.105	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	NetModule NSRW web administration interface executes an OS command constructed with unsanitized user input. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. This issue affects NSRW: from 4.3.0.0 before 4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103.	N/A	A-NET-NETM- 160323/370

0-1

1-2

3-4 4-5 2-3 Page 200 of 859

5-6

6-7

7-8

8-9

2-3 Page **201** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			privileges. This issue affects NSRW: from 4.3.0.0 before 4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103. CVE ID : CVE-2023- 0861				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	8.8	The NetModule NSRW web administration interface is vulnerable to path traversals, which could lead to arbitrary file uploads and deletion. By uploading malicious files to the web root directory, authenticated users could gain remote command execution with elevated privileges. This issue affects NSRW: from 4.3.0.0 before 4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103. CVE ID : CVE-2023- 0862	https://share. netmodule.co m/public/syst em- software/4.7/ 4.7.0.103/NRS W-RN- 4.7.0.103.pdf	A-NET-NETM- 160323/373		
Vendor: net	Vendor: networktocode						
Product: na	utobot						

0-1

1-2

2-3

3-4 4-5 Page **202** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): * Up to	(excludin	g) 1.5.7		
N/A	21-Feb-2023	9.8	Nautobot is a Network Source of Truth and Network Automation Platform. All users of Nautobot versions earlier than 1.5.7 are impacted by a remote code execution vulnerability. Nautobot did not properly sandbox Jinja2 template rendering. In Nautobot 1.5.7 has enabled sandboxed environments for the Jinja2 template engine used internally for template rendering for the following objects: 'extras.ComputedFiel d', 'extras.CustomLink', 'extras.ExportTempl ate`, 'extras.Secret`, 'extras.Webhook`. While no active exploits of this vulnerability are known this change has been made as a preventative measure to protect against any potential remote code execution attacks utilizing maliciously crafted template code. This change	https://github .com/nautobo t/nautobot/co mmit/d47f15 7e83b0c353b b2b697f9118 82c71cf90ca0, https://github .com/nautobo t/nautobot/se curity/advisor ies/GHSA- 8mfq-f5wj- vw5m	A-NET-NAUT- 160323/374

0-1

1-2

2-3

3-4 4-5 Page **203** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			forces the Jinja2		
			template engine to		
			use a		
			`SandboxedEnviron		
			ment` on all new		
			installations of		
			Nautobot. This		
			addresses any		
			potential unsafe code		
			execution		
			everywhere the		
			helper function		
			`nautobot.utilities.uti		
			ls.render_jinja2` is		
			called. Additionally,		
			the documentation		
			that had previously		
			suggesting the direct		
			use of		
			`jinja2.Template` has		
			been revised to		
			suggest		
			`render_jinja2`. Users		
			are advised to		
			upgrade to Nautobot		
			1.5.7 or newer. For		
			users that are unable		
			to upgrade to the		
			latest release of		
			Nautobot, you may		
			add the following		
			setting to your		
			`nautobot_config.py`		
			to apply the sandbox		
			environment		
			enforcement:		
			`TEMPLATES[1]["OP		
			TIONS"]["environme		
			nt"] =		
			"jinja2.sandbox.Sand		
			boxedEnvironment"`		
			After applying this		
			change, you must		
			restart all Nautobot		

0-1

1-2

2-33-44-5Page 204 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			services, including		
			any Celery worker		
			processes. **Note:**		
			*Nautobot specifies		
			two template		
			engines by default,		
			the first being		
			"django" for the		
			Django built-in		
			template engine, and		
			the second being		
			"jinja" for the Jinja2		
			template engine.		
			This recommended		
			setting will update		
			the second item in		
			the list of template		
			engines, which is the		
			Jinja2 engine.* For		
			users that are unable		
			to immediately		
			update their		
			configuration such as		
			if a Nautobot service		
			restart is too		
			disruptive to		
			operations, access to		
			provide custom		
			Jinja2 template		
			values may be		
			mitigated using		
			permissions to		
			restrict "change"		
			(write) actions to the		
			affected object types listed in the first		
			section. **Note:**		
			*This solution is		
			intended to be		
			stopgap until you can		
			successfully update		
			your		
			`nautobot_config.py`		
			or upgrade your		
			or upgraue your		

0-1

1-2

2-33-44-5Page 205 of 859

6-7

7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Nautobot instance to apply the sandboxed environment enforcement.*		
			CVE ID : CVE-2023- 25657		
Vendor: Nex	xtcloud				
Product: ne	extcloud_server				
Affected Ver	sion(s): * Up to	(excluding			
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.5	Nextcloud server is a self hosted home cloud product. In affected versions the `OC\Files\Node\Fold er::getFullPath()` function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths outside of ones own space and overwriting data from other users with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue. CVE ID : CVE-2023- 25579	https://github .com/nextclou d/server/pull /35074, https://github .com/nextclou d/security- advisories/sec urity/advisori es/GHSA- 273v-9h7x- p68v	A-NEX-NEXT- 160323/375

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 25.0.0				
N/A	25-Feb-2023	7.5	Nextcloud is an Open Source private cloud software. Versions 24.0.4 and above, prior to 24.0.7, and 25.0.0 and above, prior to 25.0.1, contain Improper Access Control. Secure view for internal shares can be circumvented if reshare permissions are also given. This issue is patched in versions 24.0.7 and 25.0.1. No workaround is available. CVE ID : CVE-2023- 25821	https://github .com/nextclou d/security- advisories/sec urity/advisori es/GHSA- 7w6h-5qgw- 4j94, https://github .com/nextclou d/server/pull /34502	A-NEX-NEXT- 160323/376
Affected Ver	sion(s): From (i	ncluding)	20.0.0 Up to (excluding) 20.0.14	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.5	Nextcloud server is a self hosted home cloud product. In affected versions the `OC\Files\Node\Fold er::getFullPath()` function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths outside of ones own space and overwriting data from other users	https://github .com/nextclou d/server/pull /35074, https://github .com/nextclou d/security- advisories/sec urity/advisori es/GHSA- 273v-9h7x- p68v	A-NEX-NEXT- 160323/377

0-1

1-2

2-3

3-4 4-5 Page **207** of **859** 5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue. CVE ID : CVE-2023- 25579		
Affected Ver	sion(s): From (i	ncluding)	21.0.0 Up to (excluding) 21.0.9	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.5	Nextcloud server is a self hosted home cloud product. In affected versions the `OC\Files\Node\Fold er::getFullPath()` function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths outside of ones own space and overwriting data from other users with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue.	https://github .com/nextclou d/server/pull /35074, https://github .com/nextclou d/security- advisories/sec urity/advisori es/GHSA- 273v-9h7x- p68v	A-NEX-NEXT- 160323/378

0-1

1-2

2-3

3-4 4-5 Page **208** of **859** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25579		
Affected Ver	sion(s): From (i	ncluding)	22.2.0 Up to (excluding) 22.2.10	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.5	Nextcloud server is a self hosted home cloud product. In affected versions the `OC\Files\Node\Fold er::getFullPath()` function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths outside of ones own space and overwriting data from other users with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue. CVE ID : CVE-2023- 25579	https://github .com/nextclou d/server/pull /35074, https://github .com/nextclou d/security- advisories/sec urity/advisori es/GHSA- 273v-9h7x- p68v	A-NEX-NEXT- 160323/379
	sion(s): From (i	ncluding)	23.0.0 Up to (excluding	-	
Improper Limitation of a Pathname to a Restricted	22-Feb-2023	7.5	Nextcloud server is a self hosted home cloud product. In affected versions the `OC\Files\Node\Fold er::getFullPath()`	https://github .com/nextclou d/server/pull /35074, https://github .com/nextclou	A-NEX-NEXT- 160323/380

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths outside of ones own space and overwriting data from other users with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue. CVE ID : CVE-2023- 25579	d/security- advisories/sec urity/advisori es/GHSA- 273v-9h7x- p68v	
Affected Ver	<mark>sion(s): From (</mark> i	ncluding)	24.0.0 Up to (excluding) 24.0.8	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.5	Nextcloud server is a self hosted home cloud product. In affected versions the `OC\Files\Node\Fold er::getFullPath()` function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths	https://github .com/nextclou d/server/pull /35074, https://github .com/nextclou d/security- advisories/sec urity/advisori es/GHSA- 273v-9h7x- p68v	A-NEX-NEXT- 160323/381

0-1

1-2

2-3

3-4 4-5 Page **210** of **859** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			outside of ones own space and overwriting data from other users with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue. CVE ID : CVE-2023- 25579		
Affected Ver	sion(s): From (i	ncluding)	24.0.4 Up to (excluding) 24.0.7	
N/A	25-Feb-2023	7.5	Nextcloud is an Open Source private cloud software. Versions 24.0.4 and above, prior to 24.0.7, and 25.0.0 and above, prior to 25.0.1, contain Improper Access Control. Secure view for internal shares can be circumvented if reshare permissions are also given. This issue is patched in versions 24.0.7 and 25.0.1. No workaround is available. CVE ID : CVE-2023- 25821	https://github .com/nextclou d/security- advisories/sec urity/advisori es/GHSA- 7w6h-5qgw- 4j94, https://github .com/nextclou d/server/pull /34502	A-NEX-NEXT- 160323/382
Affected Ver	sion(s): From (i	ncluding)	25.0.0 Up to (excluding) 25.0.2	1
Improper Limitation of a	22-Feb-2023	7.5	Nextcloud server is a self hosted home cloud product. In	https://github .com/nextclou d/server/pull	A-NEX-NEXT- 160323/383

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
Pathname to a Restricted Directory ('Path Traversal')			affected versions the `OC\Files\Node\Fold er::getFullPath()` function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths outside of ones own space and overwriting data from other users with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue. CVE ID : CVE-2023- 25579	/35074, https://github .com/nextclou d/security- advisories/sec urity/advisori es/GHSA- 273v-9h7x- p68v	
Affected Ver	sion(s): From (i	ncluding)	25.0.0 Up to (excluding) 25.0.3	
Uncontroll ed Resource Consumpti on	25-Feb-2023	6.5	Nextcloud is an Open Source private cloud software. Versions 25.0.0 and above, prior to 25.0.3, are subject to Uncontrolled Resource Consumption. A user can configure a very long password, consuming more resources on	https://github .com/nextclou d/security- advisories/sec urity/advisori es/GHSA- 53q2-cm29- 7j83, https://github .com/nextclou d/server/pull /35965	A-NEX-NEXT- 160323/384

0-1

1-2

2-3 3-4 4-5 Page **212** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
	xtcloud_talk sion(s): From (i	ncluding)	password validation than desired. This issue is patched in 25.0.3 No workaround is available. CVE ID : CVE-2023- 25816 15.0.0 Up to (excluding) 15.0.3	
Exposure of Resource to Wrong Sphere	27-Feb-2023	4.3	Nextcloud Talk is a fully on-premises audio/video and chat communication service. When cron jobs were misconfigured and therefore messages are not expired, the API would still return them while they were then hidden by the frontend code. It is recommended that the Nextcloud Talk is upgraded to 15.0.3. There are no workaround available. CVE ID : CVE-2023- 26041	https://github .com/nextclou d/spreed/pull /8515, https://github .com/nextclou d/security- advisories/sec urity/advisori es/GHSA- j53p-r755- v4jf	A-NEX-NEXT- 160323/385
Vendor: nic					•
Product: kn	sion(s): * Up to	(excluding	g) 5.6.0		
Allocation of Resources Without Limits or Throttling	21-Feb-2023	7.5	Knot Resolver before 5.6.0 enables attackers to consume its resources, launching amplification attacks	https://www. knot- resolver.cz/20 23-01-26- knot-resolver- 5.6.0.html	A-NIC-KNOT- 160323/386
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3 3-4 4-5 5</mark> Page 213 of 859	<mark>-6 6-7 7-</mark> {	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and potentially causing a denial of service. Specifically, a single client query may lead to a hundred TCP connection attempts if a DNS server closes connections without providing a response. CVE ID : CVE-2023- 26249		
Vendor: No	dejs				
Product: no	de.js				
Affected Ver	sion(s): From (i	ncluding)	14.0.0 Up to (excluding) 14.21.3	
Incorrect Authorizati on	23-Feb-2023	7.5	A privilege escalation vulnerability exists in Node.js <19.6.1, <18.14.1, <16.19.1 and <14.21.3 that made it possible to bypass the experimental Permissions (https://nodejs.org/ api/permissions.htm l) feature in Node.js and access non authorized modules by using process.mainModule. require(). This only affects users who had enabled the experimental permissions option withexperimental- policy. CVE ID : CVE-2023- 23918	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/387

0-1

1-2

2-3 3-4 4-5 Page **214** of **859** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Feb-2023	7.5	A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service. CVE ID : CVE-2023- 23919	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/388
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges. CVE ID : CVE-2023- 23920	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/389
Affected Ver	sion(s): From (i	ncluding)	14.0.0 Up to (including		
Incorrect Authorizati on	23-Feb-2023	7.5	A privilege escalation vulnerability exists in Node.js <19.6.1, <18.14.1, <16.19.1	https://nodej s.org/en/blog /vulnerability /february- 2023-	A-NOD-NODE- 160323/390

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and <14.21.3 that made it possible to bypass the experimental Permissions (https://nodejs.org/ api/permissions.htm l) feature in Node.js and access non authorized modules by using process.mainModule. require(). This only affects users who had enabled the experimental permissions option withexperimental- policy. CVE ID : CVE-2023- 23918	security- releases/	
N/A	23-Feb-2023	7.5	A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service. CVE ID : CVE-2023- 23919	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/391

0-1

1-2

2-33-44-5Page 216 of 859

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges. CVE ID : CVE-2023- 23920	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/392
Affected Ver	sion(s): From (i	ncluding)	16.0.0 Up to (excluding) 16.19.1	
Incorrect Authorizati on	23-Feb-2023	7.5	A privilege escalation vulnerability exists in Node.js <19.6.1, <18.14.1, <16.19.1 and <14.21.3 that made it possible to bypass the experimental Permissions (https://nodejs.org/ api/permissions.htm l) feature in Node.js and access non authorized modules by using process.mainModule. require(). This only affects users who had enabled the experimental permissions option withexperimental- policy. CVE ID : CVE-2023- 23918	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/393

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Feb-2023	7.5	A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service. CVE ID : CVE-2023- 23919	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/394
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	16-Feb-2023	5.4	Undici is an HTTP/1.1 client for Node.js. Starting with version 2.0.0 and prior to version 5.19.1, the undici library does not protect `host` HTTP header from CRLF injection vulnerabilities. This issue is patched in Undici v5.19.1. As a workaround, sanitize the `headers.host` string before passing to undici. CVE ID : CVE-2023- 23936	https://github .com/nodejs/ undici/commi t/a2eff05401 358f6595138 df963837c24 348f2034, https://github .com/nodejs/ undici/securit y/advisories/ GHSA-5r9g- qh6m-jxff	A-NOD-NODE- 160323/395

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges. CVE ID : CVE-2023- 23920	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/396
Affected Ver	sion(s): From (i	ncluding)	16.0.0 Up to (including) 16.12.0	
Incorrect Authorizati on	23-Feb-2023	7.5	A privilege escalation vulnerability exists in Node.js <19.6.1, <18.14.1, <16.19.1 and <14.21.3 that made it possible to bypass the experimental Permissions (https://nodejs.org/ api/permissions.htm l) feature in Node.js and access non authorized modules by using process.mainModule. require(). This only affects users who had enabled the experimental permissions option withexperimental- policy. CVE ID : CVE-2023- 23918	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/397

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Feb-2023	7.5	A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service. CVE ID : CVE-2023- 23919	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/398
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges. CVE ID : CVE-2023- 23920	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/399
Affected Ver	sion(s): From (i	ncluding)	18.0.0 Up to (excluding	-	
Incorrect Authorizati on	23-Feb-2023	7.5	A privilege escalation vulnerability exists in Node.js <19.6.1, <18.14.1, <16.19.1	https://nodej s.org/en/blog /vulnerability /february- 2023-	A-NOD-NODE- 160323/400

CVSS Scoring Scale 0-1 1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and <14.21.3 that made it possible to bypass the experimental Permissions (https://nodejs.org/ api/permissions.htm I) feature in Node.js and access non authorized modules by using process.mainModule. require(). This only affects users who had enabled the experimental permissions option withexperimental- policy. CVE ID : CVE-2023- 23918	security- releases/	
N/A	23-Feb-2023	7.5	A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service. CVE ID : CVE-2023- 23919	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/401

0-1

1-2

2-3 3-4 4-5 Page **221** of **859** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	16-Feb-2023	5.4	Undici is an HTTP/1.1 client for Node.js. Starting with version 2.0.0 and prior to version 5.19.1, the undici library does not protect `host` HTTP header from CRLF injection vulnerabilities. This issue is patched in Undici v5.19.1. As a workaround, sanitize the `headers.host` string before passing to undici. CVE ID : CVE-2023- 23936	https://github .com/nodejs/ undici/commi t/a2eff05401 358f6595138 df963837c24 348f2034, https://github .com/nodejs/ undici/securit y/advisories/ GHSA-5r9g- qh6m-jxff	A-NOD-NODE- 160323/402
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges. CVE ID : CVE-2023- 23920	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/403
Affected Ver	sion(s): From (i	ncluding)	18.0.0 Up to (including)) 18.11.0	
Incorrect Authorizati on	23-Feb-2023	7.5	A privilege escalation vulnerability exists in Node.js <19.6.1, <18.14.1, <16.19.1 and <14.21.3 that made it possible to bypass the	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/404

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			experimental Permissions (https://nodejs.org/ api/permissions.htm l) feature in Node.js and access non authorized modules by using process.mainModule. require(). This only affects users who had enabled the experimental permissions option withexperimental- policy. CVE ID : CVE-2023- 23918		
N/A	23-Feb-2023	7.5	A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service. CVE ID : CVE-2023- 23919	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/405

0-1

1-2

2-3

3-4 4-5 Page **223** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges.	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/406
			CVE ID : CVE-2023- 23920		
Affected Ver	sion(s): From (i	ncluding)	19.0.0 Up to (excluding) 19.2.0	
N/A	23-Feb-2023	7.5	A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service. CVE ID : CVE-2023- 23919	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/407
Affected Ver	sion(s): From (i	ncluding)	19.0.0 Up to (excluding) 19.6.1	
Incorrect Authorizati on	23-Feb-2023	7.5	A privilege escalation vulnerability exists in Node.js <19.6.1,	https://nodej s.org/en/blog /vulnerability /february-	A-NOD-NODE- 160323/408

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<18.14.1, <16.19.1 and <14.21.3 that made it possible to bypass the experimental Permissions (https://nodejs.org/ api/permissions.htm l) feature in Node.js and access non authorized modules by using process.mainModule. require(). This only affects users who had enabled the experimental permissions option withexperimental- policy. CVE ID : CVE-2023- 23918	2023- security- releases/	
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	16-Feb-2023	5.4	Undici is an HTTP/1.1 client for Node.js. Starting with version 2.0.0 and prior to version 5.19.1, the undici library does not protect `host` HTTP header from CRLF injection vulnerabilities. This issue is patched in Undici v5.19.1. As a workaround, sanitize the `headers.host` string before passing to undici. CVE ID : CVE-2023- 23936	https://github .com/nodejs/ undici/commi t/a2eff05401 358f6595138 df963837c24 348f2034, https://github .com/nodejs/ undici/securit y/advisories/ GHSA-5r9g- qh6m-jxff	A-NOD-NODE- 160323/409

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges.	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	A-NOD-NODE- 160323/410
			CVE ID : CVE-2023- 23920		
Product: un	idici				
Affected Ver	sion(s): * Up to	(excluding	g) 5.19.1		
N/A	16-Feb-2023	7.5	Undici is an HTTP/1.1 client for Node.js. Prior to version 5.19.1, the `Headers.set()` and `Headers.append()` methods are vulnerable to Regular Expression Denial of Service (ReDoS) attacks when untrusted values are passed into the functions. This is due to the inefficient regular expression used to normalize the values in the `headerValueNormal ize()` utility function. This vulnerability was patched in v5.19.1. No known workarounds are available.	https://github .com/nodejs/ undici/securit y/advisories/ GHSA-r6ch- mqf9-qc9w, https://github .com/nodejs/ undici/commi t/f2324e5499 43f0b0937b0 9fb1c0c16cc7 c93abdf	A-NOD-UNDI- 160323/411

0-1

1-2

2-33-44-5Page226 of859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID : CVE-2023- 24807			
Affected Vers	sion(s): From (i	ncluding)	2.0.0 Up to (excluding)	5.19.1		
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	16-Feb-2023	5.4	Undici is an HTTP/1.1 client for Node.js. Starting with version 2.0.0 and prior to version 5.19.1, the undici library does not protect `host` HTTP header from CRLF injection vulnerabilities. This issue is patched in Undici v5.19.1. As a workaround, sanitize the `headers.host` string before passing to undici. CVE ID : CVE-2023- 23936	https://github .com/nodejs/ undici/commi t/a2eff05401 358f6595138 df963837c24 348f2034, https://github .com/nodejs/ undici/securit y/advisories/ GHSA-5r9g- qh6m-jxff	A-NOD-UNDI- 160323/412	
Vendor: not	ation-go_proje	ect			<u> </u>	
Product: not	tation-go					
Affected Vers	sion(s): 0.7.0					
Allocation of Resources Without Limits or Throttling	20-Feb-2023	7.5	notation-go is a collection of libraries for supporting Notation sign, verify, push, and pull of oci artifacts. Prior to version 1.0.0-rc.3, notation-go users will find their application using excessive memory when verifying signatures. The application will be killed, and thus availability is impacted. The	https://github .com/notaryp roject/notatio n- go/security/a dvisories/GHS A-87x9-7grx- m28v	A-NOT-NOTA- 160323/413	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						

Page 227 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			problem has been patched in the release v1.0.0-rc.3. Some workarounds are available. Users can review their own trust policy file and check if the identity string contains `=#`. Meanwhile, users should only put trusted certificates in their trust stores referenced by their own trust policy files, and make sure the `authenticity` validation is set to `enforce`. CVE ID : CVE-2023-		
			25656		
Affected Ver	sion(s): 0.8.0				
Allocation of Resources Without Limits or Throttling	20-Feb-2023	7.5	notation-go is a collection of libraries for supporting Notation sign, verify, push, and pull of oci artifacts. Prior to version 1.0.0-rc.3, notation-go users will find their application using excessive memory when verifying signatures. The application will be killed, and thus availability is impacted. The problem has been patched in the release v1.0.0-rc.3. Some workarounds	https://github .com/notaryp roject/notatio n- go/security/a dvisories/GHS A-87x9-7grx- m28v	A-NOT-NOTA- 160323/414

0-1

1-2

2-3

3-4 4-5 Page **228** of **859** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are available. Users can review their own trust policy file and check if the identity string contains `=#`. Meanwhile, users should only put trusted certificates in their trust stores referenced by their own trust policy files, and make sure the `authenticity` validation is set to `enforce`.		
			CVE ID : CVE-2023- 25656		
Affected Ver	sion(s): 0.9.0			L	
Allocation of Resources Without Limits or Throttling	20-Feb-2023	7.5	notation-go is a collection of libraries for supporting Notation sign, verify, push, and pull of oci artifacts. Prior to version 1.0.0-rc.3, notation-go users will find their application using excessive memory when verifying signatures. The application will be killed, and thus availability is impacted. The problem has been patched in the release v1.0.0-rc.3. Some workarounds are available. Users can review their own trust policy file and check if the identity	https://github .com/notaryp roject/notatio n- go/security/a dvisories/GHS A-87x9-7grx- m28v	A-NOT-NOTA- 160323/415

0-1

1-2

2-33-44-5Page 229 of 859

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			string contains `=#`. Meanwhile, users should only put trusted certificates in their trust stores referenced by their own trust policy files, and make sure the `authenticity` validation is set to `enforce`. CVE ID : CVE-2023- 25656				
Vendor: not	tepadproject	:		<u> </u>			
Product: no	tepad						
Affected Ver	sion(s): 1.22						
Improper Resource Shutdown or Release	18-Feb-2023	5.5	A vulnerability, which was classified as problematic, was found in cxasm notepad 1.22. This affects an unknown part of the component Directory Comparison Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The associated identifier of this vulnerability is VDB- 221475. CVE ID : CVE-2023- 0909	N/A	A-NOT-NOTE- 160323/416		
Vendor: nuxt							
Product: nuxt							
Affected Ver	sion(s): * Up to	(excluding	g) 3.2.1				

0-1

1-2

2-3

3-4 4-5 Page **230** of **859** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	6.1	Cross-site Scripting (XSS) - Generic in GitHub repository nuxt/framework prior to 3.2.1. CVE ID : CVE-2023- 0878	https://github .com/nuxt/fra mework/com mit/7aa35ff9 58eec0c7d07 1d3fcd481db 57281dbcd9, https://huntr. dev/bounties/ a892caf7- b8c2-4638- 8cee- eb779d51066 a	A-NUX-NUXT- 160323/417
Vendor: ole	vmedia			I	L
Product: ole	evmedia_short	codes			
Affected Ver	sion(s): * Up to	(including	g) 1.1.9		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	The Olevmedia Shortcodes WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. CVE ID : CVE-2023- 0168	N/A	A-OLE-OLEV- 160323/418
	ine_boat_reser	-			
Affected Ver	line_boat_rese	rvation_s	ystem		
Improper Neutralizat	24-Feb-2023	6.1	A vulnerability has been found in	N/A	A-ONL-ONLI- 160323/419
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 231 of 859	- <mark>6 6-7 7-</mark> 8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			SourceCodester Online Boat Reservation System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /boat/login.php of the component POST Parameter Handler. The manipulation of the argument un leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB- 221755. CVE ID : CVE-2023- 1030		
			n_system_project		
	line_catering_	reservatio	on_system		
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	28-Feb-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Online Catering Reservation System 1.0. This affects an unknown part of the file /reservation/add_m essage.php of the component POST	N/A	A-ONL-ONLI- 160323/420

0-1

1-2

2-33-44-5Page232 of859

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Parameter Handler. The manipulation of the argument fullname leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB- 222003.		
			CVE ID : CVE-2023- 1100		
Vendor: online_eyewear_shop_project					
Product: online_eyewear_shop					
Affected Version(s): 1.0					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	22-Feb-2023	8.8	A vulnerability classified as problematic was found in SourceCodester Online Eyewear Shop 1.0. Affected by this vulnerability is an unknown functionality of the file admin/?page=orders /view_order. The manipulation of the argument id leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this	N/A	A-ONL-ONLI- 160323/421

0-1

1-2

2-33-44-5Page233of859

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description &	CVE ID		Patch		NCIIPC	ID
			vulnerability i 221635. CVE ID : CVE- 0966						
Vendor: onl	ine_graduate_t	tracer_sy	stem_project						
Product: on	line_graduate_	tracer_sy	vstem						
Affected Vers	sion(s): 1.0				T				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	26-Feb-2023	9.8	A vulnerability which was cla as critical, has found in SourceCodeste Online Gradua Tracer System Affected by th is some unkno functionality of file tracking/adm _acc.php. The manipulation argument id le sql injection. The attack may be launched rem The exploit has disclosed to th public and ma used. VDB-222 the identifier assigned to th vulnerability. CVE ID : CVE- 1040	ssified been er ate 1.0. is issue own of the in/add of the eads to The otely. as been ne by be 1798 is is	N/A	A		-ONL-ON 60323/4	
	ine_pet_shop_v		roject						
Product: online_pet_shop_we_app									
Affected Vers Improper Neutralizat ion of Input	sion(s): 1.0 26-Feb-2023	6.1	A vulnerabilit been found in SourceCodest Online Pet Sho	er	N/A	A		-ONL-ON 60323/4	
CVSS Scoring S	icale 0-1	1-2 2	- 3 3-4 4 Page 234 of 8 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')			App 1.0 and classified as problematic. This vulnerability affects unknown code of the file /pet_shop/admin/or ders/update_status.p hp. The manipulation of the argument oid with the input 1"> <script>alert(111 1)</script> leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221800. CVE ID : CVE-2023- 1042		
Vendor: onl	ine_pizza_orde	ering_syst	-		
	line_pizza_ord				
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	9.8	A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. This vulnerability affects unknown code of the file /php- opos/index.php. The manipulation of the argument ID leads to sql injection. The attack can be	N/A	A-ONL-ONLI- 160323/424

0-1

1-2

2-33-44-5Page 235 of 859

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. VDB-221350 is the identifier assigned to this vulnerability. CVE ID : CVE-2023- 0883		
Missing Authentica tion for Critical Function	18-Feb-2023	9.8	A vulnerability classified as critical was found in SourceCodester Online Pizza Ordering System 1.0. Affected by this vulnerability is the function delete_category of the file ajax.php of the component POST Parameter Handler. The manipulation leads to missing authentication. The attack can be launched remotely. The associated identifier of this vulnerability is VDB- 221455. CVE ID : CVE-2023- 0906	N/A	A-ONL-ONLI- 160323/425
Improper Neutralizat ion of Special Elements used in an SQL Command	18-Feb-2023	9.8	A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. This vulnerability affects unknown code of the	N/A	A-ONL-ONLI- 160323/426

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			file view_prod.php of the component GET Parameter Handler. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The identifier of this vulnerability is VDB- 221476. CVE ID : CVE-2023- 0910		
Cross-Site Request Forgery (CSRF)	23-Feb-2023	8.8	A vulnerability, which was classified as problematic, has been found in SourceCodester Online Pizza Ordering System 1.0. This issue affects some unknown processing of the file admin/ajax.php?acti on=save_user. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB- 221681 was assigned to this vulnerability. CVE ID : CVE-2023- 0988	N/A	A-ONL-ONLI- 160323/427
Improper Neutralizat ion of Input	23-Feb-2023	5.4	A vulnerability classified as problematic was found in	N/A	A-ONL-ONLI- 160323/428

0-1

1-2

2-3

3-4 4-5 Page 237 of 859

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			SourceCodester Online Pizza Ordering System 1.0. This vulnerability affects unknown code of the file index.php?page=che ckout. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB- 221680. CVE ID : CVE-2023- 0987		
Vendor: onl	line_reviewer_	managem	ient_system_project		
	line_reviewer_				
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	26-Feb-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Online Reviewer Management System 1.0. Affected is an unknown function of the file /reviewer_0/admins /assessments/pretes t/questions- view.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely.	N/A	A-ONL-ONLI- 160323/429

0-1

1-2

2-33-44-5Page238 of 859

5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221796.			
			CVE ID : CVE-2023- 1038			
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	28-Feb-2023	7.2	An issue was discovered in Online Reviewer Management System v1.0. There is a SQL injection that can directly issue instructions to the background database system via reviewer_0/admins/ assessments/course /course-update.php. CVE ID : CVE-2023-	N/A	A-ONL-ONLI- 160323/430	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	28-Feb-2023	4.8	25432 An issue was discovered in Online Reviewer Management System v1.0. There is a XSS vulnerability via reviewer_0/admins/ assessments/course /course-update.php. CVE ID : CVE-2023- 25431	N/A	A-ONL-ONLI- 160323/431	
Vendor: onl	ine_services_p	roject		I		
Product: online_services						
Affected Version(s): * Up to (excluding) 1.17						
Improper Neutralizat ion of Special	23-Feb-2023	9.8	Improper Neutralization of Special Elements used in an SQL	N/A	A-ONL-ONLI- 160323/432	
		4 2				
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-	8 8-9 <mark>9-1</mark> 0	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			Command ('SQL Injection') vulnerability in NTN Information Technologies Online Services Software allows SQL Injection.This issue affects Online Services Software: before 1.17. CVE ID : CVE-2023- 0939		
Vendor: on	line_student_m	anageme	ent_system_project		
	line_student_n				
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	28-Feb-2023	9.8	A vulnerability was found in SourceCodester Online Student Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file eduauth/edit- class-detail.php. The manipulation of the argument editid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-222002 is the identifier assigned to this vulnerability. CVE ID : CVE-2023- 1099	N/A	A-ONL-ONLI- 160323/433

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Vendor: Op	en-emr						
Product: op	Product: openemr						
Affected Ver	sion(s): * Up to	(excluding	g) 7.0.0				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	8.8	A Local File Inclusion (LFI) vulnerability in interface/forms/LBF /new.php in OpenEMR < 7.0.0 allows remote authenticated users to execute code via the formname parameter. CVE ID : CVE-2023- 22973	https://www. open- emr.org/wiki/ index.php/Op enEMR_Patch es#7.0.0_Patc h2811.2F30. 2F22.29	A-OPE-OPEN- 160323/434		
Files or Directories Accessible to External Parties	22-Feb-2023	7.5	A Path Traversal in setup.php in OpenEMR < 7.0.0 allows remote unauthenticated users to read arbitrary files by controlling a connection to an attacker-controlled MySQL server. CVE ID : CVE-2023- 22974	https://www. open- emr.org/wiki/ index.php/Op enEMR_Patch es#7.0.0_Patc h2811.2F30. 2F22.29	A-OPE-OPEN- 160323/435		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	22-Feb-2023	5.4	A Reflected Cross- site scripting (XSS) vulnerability in interface/forms/eye_ mag/php/eye_mag_f unctions.php in OpenEMR < 7.0.0 allows remote authenticated users to inject arbitrary web script or HTML via the REQUEST_URI.	https://www. open- emr.org/wiki/ index.php/Op enEMR_Patch es#7.0.0_Patc h2811.2F30. 2F22.29	A-OPE-OPEN- 160323/436		

0-1

1-2

2-3

3-4 4-5 Page **241** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22972		
Vendor: ope	encats				
Product: op	encats				
Affected Ver	sion(s): 0.9.6				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	28-Feb-2023	6.1	Improper neutralization of input during web page generation allows an unauthenticated attacker to submit malicious Javascript as the answer to a questionnaire which would then be executed when an authenticated user reviews the candidate's submission. This could be used to steal other users' cookies and force users to make actions without their knowledge. CVE ID : CVE-2023- 27293	N/A	A-OPE-OPEN- 160323/437
URL Redirectio n to Untrusted Site ('Open Redirect')	28-Feb-2023	5.4	An open redirect vulnerability exposes OpenCATS to template injection due to improper validation of user- supplied GET parameters. CVE ID : CVE-2023- 27292	N/A	A-OPE-OPEN- 160323/438
Improper Neutralizat	28-Feb-2023	5.4	Improper neutralization of	N/A	A-OPE-OPEN- 160323/439

0-1

1-2

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
ion of Input During Web Page Generation ('Cross-site Scripting')			input during web page generation allows an authenticated attacker with access to a restricted account to submit malicious Javascript as the description for a calendar event, which would then be executed in other users' browsers if they browse to that event. This could result in stealing session tokens from users with higher permission levels or forcing users to make actions without their knowledge. CVE ID : CVE-2023- 27294			
Cross-Site Request Forgery (CSRF)	28-Feb-2023	5.4	Cross-site request forgery is facilitated by OpenCATS failure to require CSRF tokens in POST requests. An attacker can exploit this issue by creating a dummy page that executes Javascript in an authenticated user's session when visited. CVE ID : CVE-2023- 27295	N/A	A-OPE-OPEN- 160323/440	
Vendor: Opennms						
Product: horizon						
Affected Version(s): * Up to (excluding) 31.0.4						
CVSS Scoring S	cale 0-1	1-2 2	2- 3 3-4 4-5 5	6-6 6-7 7	-8 8-9 9-10	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Informatio n into Log File	23-Feb-2023	6.5	Potential Insertion of Sensitive Information into Jetty Log Files in multiple versions of OpenNMS Meridian and Horizon could allow disclosure of usernames and passwords if the logging level is set to debug. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. CVE ID : CVE-2023- 0815	https://github .com/OpenNM S/opennms/p ull/5741/files	A-OPE-HORI- 160323/441
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	22-Feb-2023	6.1	Unauthenticated, stored cross-site scripting in the display of alarm reduction keys in multiple versions of OpenNMS Horizon and Meridian could allow an attacker access to confidential session information. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4.	https://github .com/OpenNM S/opennms/p ull/5506/files	A-OPE-HORI- 160323/442

0-1

1-2

2-3

3-4 4-5 Page **244** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. CVE ID : CVE-2023- 0846		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2023	6.1	Multiple stored and reflected cross-site scripting vulnerabilities in webapp jsp pages in multiple versions of OpenNMS Meridian and Horizon could allow an attacker access to confidential session information. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. CVE ID : CVE-2023- 0867	https://github .com/OpenNM S/opennms/p ull/5765	A-OPE-HORI- 160323/443

0-1

1-2

2-33-44-5Page 245 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2023	6.1	Reflected cross-site scripting in graph results in multiple versions of OpenNMS Meridian and Horizon could allow an attacker access to steal session cookies. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. CVE ID : CVE-2023- 0868	https://github .com/OpenNM S/opennms/p ull/5740	A-OPE-HORI- 160323/444
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2023	6.1	Cross-site scripting in outage/list.htm in multiple versions of OpenNMS Meridian and Horizon allows an attacker access to confidential session information. The solution is to upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4 or newer. Meridian and Horizon installation instructions state that they are intended for	https://github .com/OpenNM S/opennms/p ull/5734	A-OPE-HORI- 160323/445

0-1

1-2

2-3

3-4 4-5 Page **246** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			installation within an organization's private networks and should not be directly accessible from the Internet.		
			CVE ID : CVE-2023- 0869		
Product: me		() <u>)</u>	202240		
Affected Ver	sion(s): * Up to	excluding	g) 2023.1.0 Potential Insertion of		
Insertion of Sensitive Informatio n into Log File	23-Feb-2023	6.5	Sensitive Information into Jetty Log Files in multiple versions of OpenNMS Meridian and Horizon could allow disclosure of usernames and passwords if the logging level is set to debug. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. CVE ID : CVE-2023- 0815	https://github .com/OpenNM S/opennms/p ull/5741/files	A-OPE-MERI- 160323/446
Improper Neutralizat ion of Input	22-Feb-2023	6.1	Unauthenticated, stored cross-site scripting in the display of alarm	https://github .com/OpenNM S/opennms/p ull/5506/files	A-OPE-MERI- 160323/447

0-1

1-2

2-3

3-4 4-5 Page **247** of **859** 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			reduction keys in multiple versions of OpenNMS Horizon and Meridian could allow an attacker access to confidential session information. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. CVE ID : CVE-2023- 0846		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2023	6.1	Multiple stored and reflected cross-site scripting vulnerabilities in webapp jsp pages in multiple versions of OpenNMS Meridian and Horizon could allow an attacker access to confidential session information. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. Meridian and Horizon installation instructions state that they are	https://github .com/OpenNM S/opennms/p ull/5765	A-OPE-MERI- 160323/448

0-1

1-2

2-3

3-4 4-5 Page **248** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intended for installation within an organization's private networks and should not be directly accessible from the Internet.		
			CVE ID : CVE-2023- 0867		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2023	6.1	Reflected cross-site scripting in graph results in multiple versions of OpenNMS Meridian and Horizon could allow an attacker access to steal session cookies. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. CVE ID : CVE-2023- 0868	https://github .com/OpenNM S/opennms/p ull/5740	A-OPE-MERI- 160323/449
Improper Neutralizat ion of Input During Web Page Generation	23-Feb-2023	6.1	Cross-site scripting in outage/list.htm in multiple versions of OpenNMS Meridian and Horizon allows an attacker access to confidential session information. The	https://github .com/OpenNM S/opennms/p ull/5734	A-OPE-MERI- 160323/450

0-1

1-2

2-3

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			solution is to upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. CVE ID : CVE-2023- 0869		
Vendor: osge	eo				
Product: geo	onode				
Affected Vers	sion(s): * Up to	(excluding	g) 4.0.3		
Improper Restriction of XML External Entity Reference	27-Feb-2023	6.5	GeoNode is an open source platform that facilitates the creation, sharing, and collaborative use of geospatial data. GeoNode is vulnerable to an XML External Entity (XXE) injection in the style upload functionality of GeoServer leading to Arbitrary File Read. This issue has been patched in version 4.0.3.	https://github .com/GeoNod e/geonode/co mmit/2fdfe91 9f299b21f160 9bf898f9dcfde 58770ac0	A-OSG-GEON- 160323/451
			CVE ID : CVE-2023- 26043		
Product: geo	oserver				
A.CC . 1	sion(s): * Up to	(oveluding	T) 2 1 9 7		

0-1

1-2

2-3

3-4 4-5 Page **250** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. GeoServer includes support for the OGC Filter expression language and the OGC Common Query Language (CQL) as part of the Web Feature Service (WFS) and Web Map Service (WMS) protocols. CQL is also supported through the Web Coverage Service (WCS) protocol for ImageMosaic coverages. Users are advised to upgrade to either version 2.21.4, or version 2.22.2 to resolve this issue. Users unable to upgrade should disable the PostGIS Datastore *encode functions* setting to mitigate ``strEndsWith``, ``strStartsWith`` and ``PropertyIsLike `` misuse and enable the PostGIS DataStore *preparedStatement s* setting to mitigate the ``FeatureId`` misuse.	https://github .com/geoserv er/geoserver/ security/advis ories/GHSA- 7g5f-wrx8- 5ccf, https://github .com/geoserv er/geoserver/ commit/145a 8af79859028 8d270b24023 5e89c8f0b62e 1d	A-OSG-GEOS- 160323/452

0-1

1-2

2-33-44-5Page 251 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25157		
Affected Ver	sion(s): From (i	ncluding)	2.19.0 Up to (excluding) 2.19.7	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. GeoServer includes support for the OGC Filter expression language and the OGC Common Query Language (CQL) as part of the Web Feature Service (WFS) and Web Map Service (WMS) protocols. CQL is also supported through the Web Coverage Service (WCS) protocol for ImageMosaic coverages. Users are advised to upgrade to either version 2.21.4, or version 2.22.2 to resolve this issue. Users unable to upgrade should disable the PostGIS Datastore *encode functions* setting to mitigate ``strEndsWith``, ``strStartsWith`` and ``PropertyIsLike `` misuse and enable the PostGIS DataStore *preparedStatement	https://github .com/geoserv er/geoserver/ security/advis ories/GHSA- 7g5f-wrx8- 5ccf, https://github .com/geoserv er/geoserver/ commit/145a 8af79859028 8d270b24023 5e89c8f0b62e 1d	A-OSG-GEOS- 160323/453

0-1

1-2

2-33-44-5Page252 of859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			s* setting to mitigate the ``FeatureId`` misuse.		
			CVE ID : CVE-2023- 25157		
Affected Ver	sion(s): From (i	ncluding)	2.20.0 Up to (excluding) 2.20.7	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. GeoServer includes support for the OGC Filter expression language and the OGC Common Query Language (CQL) as part of the Web Feature Service (WFS) and Web Map Service (WMS) protocols. CQL is also supported through the Web Coverage Service (WCS) protocol for ImageMosaic coverages. Users are advised to upgrade to either version 2.21.4, or version 2.22.2 to resolve this issue. Users unable to upgrade should disable the PostGIS Datastore *encode functions* setting to mitigate ``strEndsWith``, ``strStartsWith`` and ``PropertyIsLike `` misuse and enable	https://github .com/geoserv er/geoserver/ security/advis ories/GHSA- 7g5f-wrx8- 5ccf, https://github .com/geoserv er/geoserver/ commit/145a 8af79859028 8d270b24023 5e89c8f0b62e 1d	A-OSG-GEOS- 160323/454

0-1

1-2

2-33-44-5Page 253 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the PostGIS DataStore *preparedStatement s* setting to mitigate the ``FeatureId`` misuse.		
			CVE ID : CVE-2023- 25157		
Affected Ver	rsion(s): From (i	ncluding)	2.21.0 Up to (excluding) 2.21.4	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. GeoServer includes support for the OGC Filter expression language and the OGC Common Query Language (CQL) as part of the Web Feature Service (WFS) and Web Map Service (WMS) protocols. CQL is also supported through the Web Coverage Service (WCS) protocol for ImageMosaic coverages. Users are advised to upgrade to either version 2.21.4, or version 2.22.2 to resolve this issue. Users unable to upgrade should disable the PostGIS Datastore *encode functions* setting to mitigate ``strEndsWith``,	https://github .com/geoserv er/geoserver/ security/advis ories/GHSA- 7g5f-wrx8- 5ccf, https://github .com/geoserv er/geoserver/ commit/145a 8af79859028 8d270b24023 5e89c8f0b62e 1d	A-OSG-GEOS- 160323/455

0-1

1-2

2-3

3-4 4-5 Page **254** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			``strStartsWith`` and ``PropertyIsLike `` misuse and enable the PostGIS DataStore *preparedStatement s* setting to mitigate the ``FeatureId`` misuse.		
			CVE ID : CVE-2023- 25157		
Affected Ver	sion(s): From (i	ncluding)	2.22.0 Up to (excluding) 2.22.2	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. GeoServer includes support for the OGC Filter expression language and the OGC Common Query Language (CQL) as part of the Web Feature Service (WFS) and Web Map Service (WMS) protocols. CQL is also supported through the Web Coverage Service (WCS) protocol for ImageMosaic coverages. Users are advised to upgrade to either version 2.21.4, or version 2.22.2 to resolve this issue. Users unable to upgrade should disable the PostGIS Datastore *encode	https://github .com/geoserv er/geoserver/ security/advis ories/GHSA- 7g5f-wrx8- 5ccf, https://github .com/geoserv er/geoserver/ commit/145a 8af79859028 8d270b24023 5e89c8f0b62e 1d	A-OSG-GEOS- 160323/456

0-1

1-2

2-33-44-5Page 255 of 859

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functions* setting to mitigate ``strEndsWith``, ``strStartsWith`` and ``PropertyIsLike `` misuse and enable the PostGIS DataStore *preparedStatement s* setting to mitigate the ``FeatureId`` misuse. CVE ID : CVE-2023- 25157		
Vendor: par	t-db_project		-0101		
Product: pa	rt-db				
Affected Ver	sion(s): From (i	ncluding)	1.0.0 Up to (excluding)	1.0.2	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	6.1	Part-DB is an open source inventory management system for your electronic components. User input was found not being properly escaped, which allowed malicious users to inject arbitrary HTML into the pages. The Content-Security- Policy forbids inline and external scripts so it is not possible to execute JavaScript code, unless in combination with other vulnerabilities. There are no workarounds, please upgrade to Pat-DB 1.0.2 or later.	https://github .com/Part- DB/Part-DB- server/securit y/advisories/ GHSA-9pmh- gmxx-rg2x, https://github .com/Part- DB/Part-DB- server/commi t/5b7f44f4eaa cad8a79bcede c32780e00d7 347099	A-PAR-PART- 160323/457

0-1

1-2

2-33-44-5Page256 of859

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 26042		
Vendor: pea	zip_project			•	
Product: pea	azip				
Affected Vers	sion(s): 9.0.0				
Allocation of Resources Without Limits or Throttling	17-Feb-2023	5.5	An issue in Giorgio Tani peazip v.9.0.0 allows attackers to cause a denial of service via the End of Archive tag function of the peazip/pea UNPEA feature.	N/A	A-PEA-PEAZ- 160323/458
			CVE ID : CVE-2023- 24785		
	irmacy_manag				
Product: ph	armacy_mana	gement_s	ystem		
Affected Vers	sion(s): 1.0				
Unrestricte d Upload of File with Dangerous Type	19-Feb-2023	9.8	A vulnerability has been found in codeprojects Pharmacy Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file add.php of the component Avatar Image Handler. The manipulation leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB- 221494 is the identifier assigned to this vulnerability.	N/A	A-PHA-PHAR- 160323/459

Page 257 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 0918		
Vendor: PH	Р				
Product: ph	p				
Affected Ver	sion(s): From (i	ncluding)	8.0.0 Up to (excluding)	8.0.28	
Allocation of Resources Without Limits or Throttling	16-Feb-2023	8.1	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, core path resolution function allocate buffer one byte too small. When resolving paths with lengths close to system MAXPATHLEN setting, this may lead to the byte after the allocated buffer being overwritten with NUL value, which might lead to unauthorized data access or modification. CVE ID : CVE-2023- 0568	https://bugs.p hp.net/bug.ph p?id=81746	A-PHP-PHP- 160323/460
Uncontroll ed Resource Consumpti on	16-Feb-2023	7.5	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, excessive number of parts in HTTP form upload can cause high resource consumption and excessive number of log entries. This can cause denial of service on the affected server by	N/A	A-PHP-PHP- 160323/461

0-1

1-2

2-3

3-4 4-5 Page **258** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			exhausting CPU resources or disk space.				
			CVE ID : CVE-2023- 0662				
Affected Version(s): From (including) 8.1.0 Up to (excluding) 8.1.16							
Allocation of Resources Without Limits or Throttling	16-Feb-2023	8.1	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, core path resolution function allocate buffer one byte too small. When resolving paths with lengths close to system MAXPATHLEN setting, this may lead to the byte after the allocated buffer being overwritten with NUL value, which might lead to unauthorized data access or modification. CVE ID : CVE-2023- 0568	https://bugs.p hp.net/bug.ph p?id=81746	A-PHP-PHP- 160323/462		
Uncontroll ed Resource Consumpti on	16-Feb-2023	7.5	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, excessive number of parts in HTTP form upload can cause high resource consumption and excessive number of log entries. This can cause denial of service on the	N/A	A-PHP-PHP- 160323/463		

0-1

1-2

2-33-44-5Page 259 of 859

6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected server by exhausting CPU resources or disk space. CVE ID : CVE-2023- 0662		
Affected Ver	sion(s): From (i	ncluding)	8.2.0 Up to (excluding)	8.2.3	
Allocation of Resources Without Limits or Throttling	16-Feb-2023	8.1	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, core path resolution function allocate buffer one byte too small. When resolving paths with lengths close to system MAXPATHLEN setting, this may lead to the byte after the allocated buffer being overwritten with NUL value, which might lead to unauthorized data access or modification. CVE ID : CVE-2023- 0568	https://bugs.p hp.net/bug.ph p?id=81746	A-PHP-PHP- 160323/464
Uncontroll ed Resource Consumpti on	16-Feb-2023	7.5	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, excessive number of parts in HTTP form upload can cause high resource consumption and excessive number of log entries. This can cause denial of	N/A	A-PHP-PHP- 160323/465

0-1

1-2

2-3

3-4 4-5 Page **260** of **859** 6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service on the affected server by exhausting CPU resources or disk space. CVE ID : CVE-2023- 0662		
Vendor: php	-saml-sp_proj	ect	0002		
Product: php					
Affected Versi	ion(s): * Up to	(excluding	g) 1.1.1		
Improper Restriction of XML External Entity Reference	21-Feb-2023	6.5	php-saml-sp before 1.1.1 and 2.x before 2.1.1 allows reading arbitrary files as the webserver user because resolving XML external entities was silently enabled via \LIBXML_DTDLOAD \LIBXML_DTDATTR. CVE ID : CVE-2023- 26267	https://git.sr. ht/~fkooman /php-saml- sp/log, https://git.sr. ht/~fkooman /php-saml- sp/commit/8 51f75b298a7 7e62d9022f1 b170f662f5f7 716d6	A-PHP-PHP 160323/466
Affected Versi	<mark>ion(s): From (i</mark>	ncluding)	2.0.0 Up to (excluding)	2.1.1	Ι
External Entity Reference	21-Feb-2023	6.5	php-saml-sp before 1.1.1 and 2.x before 2.1.1 allows reading arbitrary files as the webserver user because resolving XML external entities was silently enabled via \LIBXML_DTDLOAD \LIBXML_DTDATTR. CVE ID : CVE-2023- 26267	https://git.sr. ht/~fkooman /php-saml- sp/log, https://git.sr. ht/~fkooman /php-saml- sp/commit/8 51f75b298a7 7e62d9022f1 b170f662f5f7 716d6	A-PHP-PHP 160323/467
Vendor: Php	myfag				1

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ph	pmyfaq		I		I
Affected Ver	sion(s): * Up to	(excluding	g) 3.1.11		
Misinterpr etation of Input	17-Feb-2023	4.3	Misinterpretation of Input in GitHub repository thorsten/phpmyfaq prior to 3.1.11. CVE ID : CVE-2023- 0880	https://github .com/thorsten /phpmyfaq/c ommit/a67dc a41576834a1 ddfee61b9e79 9b686b75d4f a, https://huntr. dev/bounties/ 14fc4841- 0f5d-4e12- bf9e- 1b60d2ac6a6 c	A-PHP-PHPM- 160323/468
Vendor: Pin	ncore		L	I	L
Product: pin	mcore				
Affected Ver	sion(s): * Up to	(excluding	g) 10.5.18		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.18. CVE ID : CVE-2023- 1067	https://huntr. dev/bounties/ 31d17b34- f80d-49f2- 86e7- 97ae715cc04 5, https://github .com/pimcore /pimcore/co mmit/4b5733 266d7d6aeb4f 221a15e005d b83fc198edf	A-PIM-PIMC- 160323/469
Vendor: pix	elfed				·
Product: pix					
Affected Ver	sion(s): * Up to	(excluding	g) 0.11.4		
N/A	18-Feb-2023	5.3	Exposure of Sensitive Information to an	https://huntr. dev/bounties/ 0327b1b2-	A-PIX-PIXE- 160323/470

 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
			Unauthorized Actor in GitHub repository pixelfed/pixelfed prior to 0.11.4. CVE ID : CVE-2023- 0901	6e7c-4154- a307- 15f23657101 0, https://github .com/pixelfed /pixelfed/com mit/5b5f5bc3 8ca9ba39d0b 7dacc3813fb8 99f71ba57	
N/A	19-Feb-2023	5.3	Improper Authorization in GitHub repository pixelfed/pixelfed prior to 0.11.4. CVE ID : CVE-2023- 0914	https://github .com/pixelfed /pixelfed/com mit/ef56f92c3 d77e9bafaa70 c08b7c04d5a 61b8d454, https://huntr. dev/bounties/ 54d5fd76- e038-4eda- 9e03- d5e95e09c0ec	A-PIX-PIXE- 160323/471
Vendor: pre					
	/_sticky_eleme				
Affected Vers	sion(s): * Up to	(excluding		Γ	Γ
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	7.2	The My Sticky Elements WordPress plugin before 2.0.9 does not properly sanitise and escape a parameter before using it in a SQL statement when deleting messages, leading to a SQL injection exploitable by high privilege users such as admin CVE ID : CVE-2023- 0487	N/A	A-PRE-MY_S- 160323/472
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	<u> </u>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: PT	C	<u> </u>			I
Product: ke	pware_server				
Affected Ver	sion(s): * Up to	(including	g) 6.12		
Integer Overflow or Wraparoun d	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code. CVE ID : CVE-2023- 0754	N/A	A-PTC-KEPW- 160323/473
Improper Validation of Array Index	23-Feb-2023	9.8	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code. CVE ID : CVE-2023- 0755	N/A	A-PTC-KEPW- 160323/474
Product: ke	pware_servere	ex			
Affected Ver	sion(s): * Up to	(including	g) 6.12		
Integer Overflow or Wraparoun d	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code.	N/A	A-PTC-KEPW- 160323/475

0-1

1-2

5-6

6-7

Improper Validation ,	23-Feb-2023		CVE ID : CVE-2023- 0754 The affected products are vulnerable to an improper validation			
Validation	23-Feb-2023		products are vulnerable to an			
of Array Index		9.8	of array index, which could allow an attacker to crash the server and remotely execute arbitrary code.	N/A	A-PTC-KEPW- 160323/476	
			CVE ID : CVE-2023- 0755			
	ngworxnet-so					
Affected Versi	ion(s): * Up to	(including		r		
Integer Overflow or 2 Wraparoun d	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code.	N/A	A-PTC-THIN- 160323/477	
			CVE ID : CVE-2023- 0754			
Improper Validation of Array Index	23-Feb-2023	9.8	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code.	N/A	A-PTC-THIN- 160323/478	
			CVE ID : CVE-2023- 0755			
Product: thin	ngworx_edge_	c-sdk				
CVSS Scoring Sca	ale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Affected Vers	sion(s): * Up to	(including	g) 2.2.12.1052		•	
Integer Overflow or Wraparoun d	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code. CVE ID : CVE-2023- 0754	N/A	A-PTC-THIN- 160323/479	
Improper Validation of Array Index	23-Feb-2023	9.8	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code. CVE ID : CVE-2023-	N/A	A-PTC-THIN- 160323/480	
			0755			
	ngworx_edge_					
Affected Version(s): * Up to (including) 5.4.10.0						
Integer Overflow or Wraparoun d	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code.	N/A	A-PTC-THIN- 160323/481	
Improper Validation	23-Feb-2023	9.8	CVE ID : CVE-2023- 0754 The affected products are	N/A	A-PTC-THIN- 160323/482	
CVSS Scoring S	icale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code.		
			CVE ID : CVE-2023- 0755		
Product: thi	ingworx_indus	trial_con	nectivity		
Affected Ver	sion(s): -				
Improper Validation of Array Index	23-Feb-2023	9.8	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code. CVE ID : CVE-2023- 0755	N/A	A-PTC-THIN- 160323/483
Affected Ver	sion(s): *				
Integer Overflow or Wraparoun d	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code.	N/A	A-PTC-THIN- 160323/484
			CVE ID : CVE-2023- 0754		
Product: thi	ingworx_kepw	are_edge		l	I
Affected Ver	sion(s): * Up to	(including	g) 1.5		

0-1

1-2

2-3

3-4 4-5 Page **267** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparoun d	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code. CVE ID : CVE-2023- 0754	N/A	A-PTC-THIN- 160323/485
Improper Validation of Array Index	23-Feb-2023	9.8	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code. CVE ID : CVE-2023- 0755	N/A	A-PTC-THIN- 160323/486
Vendor: puz	zzle				
Product: lii					
Affected Ver	sion(s): * Up to	(excluding	g) 1.17.28		
Improper Neutralizat ion of Special Elements used in an Expression Language Statement ('Expressio n Language Injection')	20-Feb-2023	9.8	Liima before 1.17.28 allows server-side template injection. CVE ID : CVE-2023- 26092	https://github .com/liimaorg /liima/pull/6 78	A-PUZ-LIIM- 160323/487
Improper Neutralizat	20-Feb-2023	9.8	Liima before 1.17.28 allows Hibernate	https://github .com/liimaorg	A-PUZ-LIIM- 160323/488

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	/-8	8-9	9-10
CVCC Cooring Coolo	0.1	1 1 2	2.2	2 4		ГС	67	70	0 0	0 10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			query language (HQL) injection, related to colToSort in the deployment filter. CVE ID : CVE-2023- 26093	/liima/pull/6 63	
Vendor: Python Product: python					
Affected Version(s): * Up to (excluding) 3.11					
Improper Input Validation	17-Feb-2023	7.5	An issue in the urllib.parse component of Python before v3.11 allows attackers to bypass blocklisting methods by supplying a URL that starts with blank characters. CVE ID : CVE-2023- 24329	https://github .com/python/ cpython/pull/ 99421	A-PYT-PYTH- 160323/489
Vendor: quantumcloud					
Product: chatbot					
Affected Version(s): * Up to (excluding) 4.2.9					
Cross-Site Request Forgery (CSRF)	23-Feb-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in QuantumCloud ChatBot ? plugin <= 4.2.8 versions. CVE ID : CVE-2023- 24415	N/A	A-QUA-CHAT- 160323/490
Vendor: quarkus					
Product: quarkus					
Affected Version(s): * Up to (excluding) 2.16.1					
Exposure of	24-Feb-2023	3.3	In RestEasy Reactive implementation of	https://github .com/quarkus	A-QUA-QUAR- 160323/491
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 269 of 859					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			Quarkus the insecure File.createTempFile() is used in the FileBodyHandler class which creates temp files with insecure permissions that could be read by a local user. CVE ID : CVE-2023- 0481	io/quarkus/p ull/30694	
Affected Ver	sion(s): * Up to	(excluding	g) 2.13.7		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2023	6.1	If the Quarkus Form Authentication session cookie Path attribute is set to `/` then a cross-site attack may be initiated which might lead to the Information Disclosure. This attack can be prevented with the Quarkus CSRF Prevention feature. CVE ID : CVE-2023- 0044	N/A	A-QUA-QUAR- 160323/492
Vendor: qui	ck-plugins				
	an_comparison				
Affected Ver	sion(s): * Up to	excluding			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The Loan Comparison WordPress plugin before 1.5.3 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode	N/A	A-QUI-LOAN- 160323/493

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks CVE ID : CVE-2023-		
			0366		
Vendor: ran					
Product: ran					
Improperly Controlled Modificatio n of Object Prototype Attributes ('Prototype Pollution')	24-Feb-2023	8.2	All versions of the package rangy are vulnerable to Prototype Pollution when using the extend() function in file rangy-core.js.The function uses recursive merge which can lead an attacker to modify properties of the Object.prototype CVE ID : CVE-2023- 26102	N/A	A-RAN-RANG- 160323/494
	d_more_excer		roject		
	ad_more_excer	-	160		
Cross-Site Request Forgery (CSRF)	sion(s): * Up to 27-Feb-2023	4.3	The Download Read More Excerpt Link plugin for WordPress is vulnerable to Cross- Site Request Forgery in versions up to, and including, 1.6.0. This is due to missing or incorrect nonce validation on the	https://plugin s.trac.wordpre ss.org/change set/2871098/ read-more- excerpt- link/trunk/re ad-more- excerpt- link.php	A-REA-READ- 160323/495
		1 2 3			
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 271 of 859	<mark>-6 6-7 7-8</mark>	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read_more_excerpt_li nk_menu_options() function. This makes it possible for unauthenticated attackers to update he plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.		
			CVE ID : CVE-2023- 1068		
Vendor: real	ltimelogic				
Product: fug	uhub				
Affected Vers	sion(s): * Up to	(including	g) 8.1		
Improper Control of Generation of Code ('Code Injection')	17-Feb-2023	8.8	Real Time Logic FuguHub v8.1 and earlier was discovered to contain a remote code execution (RCE) vulnerability via the component /FuguHub/cmsdocs/	N/A	A-REA-FUGU- 160323/496
			CVE ID : CVE-2023- 24078		
Vendor: Red	lhat				
Product: bui	ild_of_quarkus	;			
Affected Vers	sion(s): -				
Improper Neutralizat ion of Input During Web Page Generation	23-Feb-2023	6.1	If the Quarkus Form Authentication session cookie Path attribute is set to `/` then a cross-site attack may be initiated which might	N/A	A-RED-BUIL- 160323/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			lead to the Information Disclosure. This attack can be prevented with the Quarkus CSRF Prevention feature. CVE ID : CVE-2023- 0044		
Product: dir	rectory_server				·
Affected Vers	sion(s): 11.5				
Improper Certificate Validation	27-Feb-2023	5.5	A flaw was found in RHDS 11 and RHDS 12. While browsing entries LDAP tries to decode the userPassword attribute instead of the userCertificate attribute which could lead into sensitive information leaked. An attacker with a local account where the cockpit- 389-ds is running can list the processes and display the hashed passwords. The highest threat from this vulnerability is to data confidentiality. CVE ID : CVE-2023- 1055	https://bugzil la.redhat.com /show_bug.cgi ?id=2173517 #c0	A-RED-DIRE- 160323/498
Affected Ver	sion(s): 11.6			l	
Improper Certificate Validation	27-Feb-2023	5.5	A flaw was found in RHDS 11 and RHDS 12. While browsing entries LDAP tries to decode the userPassword	https://bugzil la.redhat.com /show_bug.cgi ?id=2173517 #c0	A-RED-DIRE- 160323/499
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	3 8-9 <mark>9-10</mark>

Page 273 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attribute instead of the userCertificate attribute which could lead into sensitive information leaked. An attacker with a local account where the cockpit- 389-ds is running can list the processes and display the hashed passwords. The highest threat from this vulnerability is to data confidentiality.		
			CVE ID : CVE-2023- 1055		
Affected Ver	sion(s): 12.0		I	1	
Improper Certificate Validation	27-Feb-2023	5.5	A flaw was found in RHDS 11 and RHDS 12. While browsing entries LDAP tries to decode the userPassword attribute instead of the userCertificate attribute which could lead into sensitive information leaked. An attacker with a local account where the cockpit- 389-ds is running can list the processes and display the hashed passwords. The highest threat from this vulnerability is to data confidentiality.	https://bugzil la.redhat.com /show_bug.cgi ?id=2173517 #c0	A-RED-DIRE- 160323/500

0-1

1-2

2-3

3-4 4-5 Page **274** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2023- 1055					
Affected Ver	Affected Version(s): 12.1							
Improper Certificate Validation	27-Feb-2023	5.5	A flaw was found in RHDS 11 and RHDS 12. While browsing entries LDAP tries to decode the userPassword attribute instead of the userCertificate attribute which could lead into sensitive information leaked. An attacker with a local account where the cockpit- 389-ds is running can list the processes and display the hashed passwords. The highest threat from this vulnerability is to data confidentiality. CVE ID : CVE-2023- 1055	https://bugzil la.redhat.com /show_bug.cgi ?id=2173517 #c0	A-RED-DIRE- 160323/501			
Product: re	steasy							
Affected Ver	sion(s): * Up to	(excluding	g) 4.7.8					
N/A	17-Feb-2023	5.5	In RESTEasy the insecure File.createTempFile() is used in the DataSourceProvider, FileProvider and Mime4JWorkaround classes which creates temp files with insecure permissions that could be read by a local user.	https://github .com/resteasy /resteasy/pull /3409/commi ts/807d7456f 2137cde8ef7c 316707211bf 4e542d56	A-RED-REST- 160323/502			

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 0482		
Vendor: roc	ket.chat				
Product: ro	cket.chat				
Affected Vers	sion(s): * Up to	(excludin	g) 5.2.0		
Improperly Controlled Modificatio n of Object Prototype Attributes ('Prototype Pollution')	23-Feb-2023	8.8	A prototype pollution vulnerability exists in Rocket.Chat server <5.2.0 that could allow an attacker to a RCE under the admin account. Any user can create their own server in your cloud and become an admin so this vulnerability could affect the cloud infrastructure. This attack vector also may increase the impact of XSS to RCE which is dangerous for self-hosted users as well. CVE ID : CVE-2023- 23917	N/A	A-ROC-ROCK- 160323/503
Vendor: Roo	ckwellautomat	cion			
Product: ke	pserver_enter	prise			
Affected Vers	sion(s): * Up to	(including	g) 6.12		
Integer Overflow or Wraparoun d	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code.	N/A	A-ROC-KEPS- 160323/504
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5	6-6 6-7 7-6	8 8-9 9-10
2433 300 mg 3			Page 276 of 859		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 0754		
Improper Validation of Array Index	23-Feb-2023	9.8	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code. CVE ID : CVE-2023- 0755	N/A	A-ROC-KEPS- 160323/505
Vendor: ros	ariosis				
Product: ro					
Affected Ver	sion(s): * Up to	(excluding	g) 10.8.2		
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	24-Feb-2023	7.5	Improper Access Control in GitHub repository francoisjacquet/rosa riosis prior to 10.8.2. CVE ID : CVE-2023- 0994	https://github .com/francoisj acquet/rosari osis/commit/ 630d3e3d782 70db8dbcbfe8 7db265bc3e7 0c5a76, https://huntr. dev/bounties/ a281c586- 9b97-4d17- 88ff- ca91bb4c45a d	A-ROS-ROSA- 160323/506
Vendor: sal	esagility				
Product: su	itecrm				
Affected Ver	sion(s): * Up to	(excluding	g) 7.12.9		
Path Traversal: 'filename'	25-Feb-2023	8.8	Path Traversal: '\\filename' in GitHub repository salesagility/suitecrm prior to 7.12.9.	https://huntr. dev/bounties/ 0c1365bc- 8d9a-4ae0- 8b55-	A-SAL-SUIT- 160323/507

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			l	Page 277 o	of 859					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 1034	615d492b373 0, https://github .com/salesagil ity/suitecrm/ commit/c19f2 21a41706efc8 d73cef95c5e3 62c4f86bf06	
			t_system_project		
Affected Ver	les_tracker_ma	inagemer	it_system		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	22-Feb-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Sales Tracker Management System 1.0. Affected is an unknown function of the file admin/products/vie w_product.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. VDB-221634 is the identifier assigned to this vulnerability. CVE ID : CVE-2023- 0964	N/A	A-SAL-SALE- 160323/508
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	23-Feb-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Sales Tracker Management System 1.0. This affects an unknown part of the file admin/?page=user/ manage_user of the	N/A	A-SAL-SALE- 160323/509

0-1

1-2

2-3

3-4 4-5 Page **278** of **859** 6-7

5-6

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component Edit User. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB- 221679.		
			CVE ID : CVE-2023- 0986		
Cross-Site Request Forgery (CSRF)	24-Feb-2023	8.8	A vulnerability classified as problematic was found in SourceCodester Sales Tracker Management System 1.0. This vulnerability affects unknown code of the file admin/?page=user/li st. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-221734 is the identifier assigned to this vulnerability. CVE ID : CVE-2023- 0999	N/A	A-SAL-SALE- 160323/510
Vendor: san					
	sy_digital_dow		-) 2 1 0 E		
Affected Vers	sion(s): * Up to	lexcluding	3.1.0.5		

0-1

1-2

2-3

3-4 4-5 Page **279** of **859** 5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The Easy Digital Downloads WordPress plugin before 3.1.0.5 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. CVE ID : CVE-2023- 0380	N/A	A-SAN-EASY- 160323/511
Vendor: Sch	neider-electri	C			
Product: cle	earscada				
Affected Ver	sion(s): *				
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020,	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-CLEA- 160323/512

0-1

1-2

2-3 3-4 4-5 Page 280 of 859 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023-		
			0595		
Product: eco	ostruxure_geo	_scada_ex	spert_2019	<u> </u>	
Affected Ver	sion(s): -				
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, ClearSCADA Expert 2023, CVE ID : CVE-2023-	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/513
Affected Ver	sion(s): 81.726	8.1	0070		
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/514
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-	8 8-9 9-10
		2			

Page 281 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023-		
		2.4	0595		
Affected ver	sion(s): 81.7322	2.1	A CWE-117:		
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, All Versions)	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/515

0-1

1-2

2-33-44-5Page 282 of 859

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 0595		
Affected Ver	sion(s): 81.742	9.2			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, ClearSCADA (All Versions)	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/516
Affected Ver	sion(s): 81.745	7.1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/517

0-1

1-2

2-33-44-5Page 283 of 859

5-6

6-7

8-9

			(default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023- 0595		
Affected Vers	sion(s): 81.7488	3.1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, CHE H CHE	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/518

0-1

1-2

2-3

3-4 4-5 Page **284** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/519
Affected Ver	sion(s): 81.754	5 1	0595		
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019,	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/520

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023-		
			0595		
Affected Ver	sion(s): 81.757	3.1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, ClearSCADA (All Versions)	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/521
Affected Ver	sion(s): 81.761	3.1		I	
Improper Encoding or	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability	https://www. se.com/ww/e n/download/ document/SE	A-SCH-ECOS- 160323/522

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Escaping of Output			exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023- 0595	VD-2023-045- 01/	
Affected Ver	sion(s): 81.764	1.1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020,	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/523

0-1

1-2

2-33-44-5Page 287 of 859

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023-					
			0595					
Affected Ver	sion(s): 81.769	0.1		Γ				
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, CUE ID : CVE-2023- GEO SCADA Expert 2021, CUE ID : CVE-2023- CUE ID : CV	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/524			
Affected Ver	Affected Version(s): 81.7714.1							
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/525			

0-1

1-2

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023-		
		2 1	0595		
Allected ver	<mark>sion(s): 81.7742</mark>	2.1	A CWE-117:		
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, All Versions)	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/526

0-1

1-2

2-3 3-4 4-5 Page 289 of 859 5-6

6-7

7-8 8-9

9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 0595		
Affected Ver	sion(s): 81.777	7.1		•	
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, ClearSCADA (All Versions)	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/527
Affected Ver	sion(s): 81.780	8.2		·	
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/528

0-1

1-2

2-33-44-5Page 290 of 859

5-6

6-7

0-1

1-2

2-3

3-4 4-5 Page **291** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/530
Affected Ver	sion(s): 81.789	6.1	0595		
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019,	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/531

0-1

1-2

2-3

3-4 4-5 Page **292** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023-		
			0595		
Affected Ver	sion(s): 81.793	5.1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, ClearSCADA (All Versions)	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/532
Affected Ver	sion(s): 81.798	0.1		1	·
Improper Encoding or	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability	https://www. se.com/ww/e n/download/ document/SE	A-SCH-ECOS- 160323/533

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Escaping of Output			exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023- 0595	VD-2023-045- 01/	
Affected Ver	sion(s): 81.801	5.1	<u> </u>		
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020,	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/534

0-1

1-2

2-3 3-4 4-5 Page 294 of 859 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023- 0595		
Affected Ver	sion(s): 81.810	8.2	0070		
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/535
Affected Ver	sion(s): 81.8122	2.1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/536

0-1

1-2

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023- 0595		
Affected Ver	sion(s): 81.815	5.1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, ClearSCADA (All Versions)	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/537

0-1

1-2

2-33-44-5Page 296 of 859

5-6

6-7

7-8 8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 0595		
Affected Ver	sion(s): 81.817	2.1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, ClearSCADA (All Versions)	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/538
Affected Ver	sion(s): 81.819	7.1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/539

0-1

1-2

2-3

3-4 4-5 Page **297** of **859** 5-6

6-7

9-10

0-1

1-2

2-3

3-4 4-5 Page **298** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/541
Product: eco	ostruxure_geo	scada ex			
Affected Vers			•		
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/542
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 299 of 859	<mark>-6 6-7 7-</mark> 8	8-9 9-10

Page **299** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023- 0595				
Affected Ver	sion(s): 83.755	1.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, ClearSCADA (All Versions)	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/543		
	Affected Version(s): 83.7578.1						
Improper Encoding or	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for	https://www. se.com/ww/e n/download/	A-SCH-ECOS- 160323/544		

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Escaping of Output			Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023-	document/SE VD-2023-045- 01/	
Affected Vor	rion(a), 02.7(1)	2 1	0595		
Affected Ver	<mark>sion(s): 83.7613</mark>	5.1	A CWE-117:		
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/545

0-1

1-2

2-33-44-5Page 301 of 859

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions)		
			CVE ID : CVE-2023- 0595		
Affected Ver	sion(s): 83.764	1.1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, ClearSCADA (All Versions) CVE ID : CVE-2023- 0595	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/546
Affected Ver	sion(s): 83.769	2.1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/547

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023- 0595		
Affected Ver	sion(s): 83.771	7.1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, EcoStruxure Geo	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/548

0-1

1-2

2-33-44-5Page 303 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2022), ClearSCADA (All Versions) CVE ID : CVE-2023- 0595		
Affected Ver	sion(s): 83.7742	2.1	<u> </u>		<u> </u>
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023-	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/549
Affected Ver	sion(s): 83.7782	7.1	0595		
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/550

0-1

1-2

2-3

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023- 0595		
Affected Version(s): 83.7809.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions)	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/551

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2023- 0595					
Affected Ver	Affected Version(s): 83.7840.1							
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, ClearSCADA (All Versions)	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/552			
Affected Ver	sion(s): 83.787	5.1						
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/553			

0-1

1-2

2-3

3-4 4-5 Page **306** of **859** 5-6

6-7

9-10

Improper Encoding or Escaping of Output24-Feb-20235.3A CWE-117: Improper Calculation Scaper 2020, ClearSCADA (All Versions) CVE ID : CVE-2023- 0595https://www. sc.com/ww/e n/download/ document/SE VD-2023-045- 01/A-SCH-ECOS- 160323/554Improper Encoding or Cottput5.3A CWE-117: Improper Output Neuralization for Logs vulnerability exists that could cause the miniterpretation of log files when malicious packets are sent to the Geo SCADA Server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, ClearSCADA (All Versions) prior to October 2022), ClearSCADA (All Versions)https://www. sc.com/ww/e n/download/ doute the sc.com/ww/e n/download/ sc.com/ww/e n/download/ sc.com/ww/e n/download/ sc.com/ww/e n/download/ sc.com/ww/e n/download/ sc.com/ww/e n/download/ sc.com/ww/e n/download/ sc.com/ww/e n/download/ sc.com/ww/e n/download/ sc.com/ww/e n/download/ sc.com/ww/e n/download/<	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of OutputA CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443).https://www. se.com/ww/e n/download/ https://www. se.com/ww/e n/download/ https://secom/w/e 160323/55424-Feb-20235.35.3https://www. secom/ww/e Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, Clair Versions prior to October 2022), ClearSCADA (All Versions)A-SCH-ECOS- dide to the total tota				Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023-		
Improper Encoding or Escaping of Output24-Feb-20235.3Improper output Neutralization for Logs vulnerability exists that could cause the malicious packets are sent to the Geo SCADA server's database web port Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, 	Affected Vers	sion(s): 83.7913	3.1	<u> </u>		
Affected Version(s): 83.7936.2	Encoding or Escaping of Output			Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions)	se.com/ww/e n/download/ document/SE VD-2023-045-	

0-1

1-2

2-3

3-4 4-5 Page **307** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/555
Affected Ver	sion(s), 92,709	n 2	0595		
Affected Ver Improper Encoding or Escaping of Output	sion(s): 83.798	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019,	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/556

0-1

1-2

2-3

3-4 4-5 Page **308** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023-		
			0595		
Affected Ver	sion(s): 83.801	7.1	•		
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, ClearSCADA (All Versions)	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/557
Affected Ver	sion(s): 83.810	3.1		1	L
Improper Encoding or	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability	https://www. se.com/ww/e n/download/ document/SE	A-SCH-ECOS- 160323/558

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Escaping of Output			exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023- 0595	VD-2023-045- 01/	
Affected Ver	sion(s): 83.812	2.2			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020,	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/559

0-1

1-2

2-33-44-5Page 310 of 859

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023- 0595		
Affected Ver	sion(s): 83.815	5.1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/560
Affected Ver	sion(s): 83.818	1.1		•	
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/561

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023-		
		7.1	0595		
Allected ver	<mark>sion(s): 83.819</mark> 2	/.1	A CWE-117:		
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, ClearSCADA (All Versions)	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/562

0-1

1-2

2-33-44-5Page 312 of 859

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2023- 0595					
Affected Ver	Affected Version(s): 83.8221.1							
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, ClearSCADA (All Versions)	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/563			
Affected Ver	sion(s): 83.826	7.1		•				
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/564			

0-1

1-2

2-3

3-4 4-5 Page **313** of **859** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023-		
Due du et. e e		aaada ay	0595		
Affected Ver	ostruxure_geo	_scada_ex	pert_2021		
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, ClearSCADA (All Versions) CVE ID : CVE-2023- 0595	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/565

0-1

1-2

2-3 3-4 4-5 Page **314** of **859** 5-6

6-7 7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): 84.8027.1							
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/566		
Affected Ver	sion(s): 84.8108	3.1	0595				
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/567		
Ecostruxure Geo							

3-4 4-5 2-3 Page **315** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023- 0595		
Affected Ver	sion(s): 84.812).1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, ClearSCADA (All Versions)	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/568
	sion(s): 84.8158	3.1		1	
Improper Encoding or	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for	https://www. se.com/ww/e n/download/	A-SCH-ECOS- 160323/569

 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
Escaping of Output			Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023-	document/SE VD-2023-045- 01/	
Affected Ver	aion(a), 04 010	0.1	0595		
Affected Ver	<mark>sion(s): 84.818</mark> 2	2.1	A CWE-117:		
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/570

0-1

1-2

2-33-44-5Page 317 of 859

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions)		
			CVE ID : CVE-2023- 0595		
Affected Ver	sion(s): 84.819	7.1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021, All Versions CVE ID : CVE-2023- 0595	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/571
Affected Ver	sion(s): 84.821	8.1			
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/572

0-1

1-2

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) CVE ID : CVE-2023-		
Affected Ver	sion(s): 84.8269	9.1	0595		
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October	https://www. se.com/ww/e n/download/ document/SE VD-2023-045- 01/	A-SCH-ECOS- 160323/573

0-1

1-2

2-3 3-4 4-5 Page **319** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2022), ClearSCADA (All Versions)		
			CVE ID : CVE-2023- 0595		
Vendor: sea	cms				
Product: sea	acms				
Affected Ver	sion(s): 11.6			1	1
Deserializa tion of Untrusted Data	22-Feb-2023	9.8	A vulnerability was found in SeaCMS 11.6 and classified as problematic. Affected by this issue is some unknown functionality of the file /data/config.ftp.php of the component Picture Management. The manipulation leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-221630 is the identifier assigned to this vulnerability. CVE ID : CVE-2023- 0960	N/A	A-SEA-SEAC- 160323/574
Vendor: seq					
Product: see	sion(s): 7.0.0				
N/A	16-Feb-2023	9.8	Due to improper artibute filtering in the sequalize js library, can a	N/A	A-SEQ-SEQU- 160323/575

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			I	Page 320 d	of 859					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker peform SQL injections. CVE ID : CVE-2023-		
			22578		
Access of Resource Using Incompatib le Type ('Type Confusion')	16-Feb-2023	8.8	Due to improper parameter filtering in the sequalize js library, can a attacker peform injection. CVE ID : CVE-2023- 22579	N/A	A-SEQ-SEQU- 160323/576
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	16-Feb-2023	7.5	Due to improper input filtering in the sequalize js library, can malicious queries lead to sensitive information disclosure.	N/A	A-SEQ-SEQU- 160323/577
	• () * 11 +		CVE ID : CVE-2023- 22580		
Affected Vers	sion(s): * Up to	(excluding			
Access of Resource Using Incompatib le Type ('Type Confusion')	16-Feb-2023	8.8	Due to improper parameter filtering in the sequalize js library, can a attacker peform injection. CVE ID : CVE-2023- 22579	N/A	A-SEQ-SEQU- 160323/578
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	16-Feb-2023	7.5	Due to improper input filtering in the sequalize js library, can malicious queries lead to sensitive information disclosure. CVE ID : CVE-2023- 22580	N/A	A-SEQ-SEQU- 160323/579
Affected Vers	sion(s): * Up to	(excluding	g) 6.19.1	I	

0-1

1-2

2-3

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	22-Feb-2023	9.8	Sequelize is a Node.js ORM tool. In versions prior to 6.19.1 a SQL injection exploit exists related to replacements. Parameters which are passed through replacements are not properly escaped which can lead to arbitrary SQL injection depending on the specific queries in use. The issue has been fixed in Sequelize 6.19.1. Users are advised to upgrade. Users unable to upgrade should not use the `replacements` and the `where` option in the same query. CVE ID : CVE-2023- 25813	https://github .com/sequeliz e/sequelize/c ommit/ccaa3 996047fe000 48d5993ab2d d43ebadd4f78 b, https://github .com/sequeliz e/sequelize/s ecurity/advis ories/GHSA- wrh9-cjv3- 2hpw	A-SEQ-SEQU- 160323/580
Affected Ver	sion(s): * Up to	(excludin	g) 6.29.0		
N/A	16-Feb-2023	9.8	Due to improper artibute filtering in the sequalize js library, can a attacker peform SQL injections. CVE ID : CVE-2023- 22578	N/A	A-SEQ-SEQU- 160323/581
Vendor: sho	ortnixel		22370		
	ortpixel_adapt	ive imag	es		
	sion(s): * Up to	0			
Improper Neutralizat ion of	27-Feb-2023	6.1	The ShortPixel Adaptive Images WordPress plugin	N/A	A-SHO-SHOR- 160323/582

 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
Input During Web Page Generation ('Cross-site Scripting')			before 3.6.3 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against any high privilege users such as admin CVE ID : CVE-2023- 0334		
Vendor: sin	ple_customer_	_relations	ship_management_sys	tem_project	
Product: sir	nple_customer	_relation	ship_management_sys	item	
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	19-Feb-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Simple Customer Relationship Management System 1.0. This affects an unknown part of the file /php- scrm/login.php. The manipulation of the argument Password leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB- 221493 was assigned to this vulnerability. CVE ID : CVE-2023- 0917	N/A	A-SIM-SIMP- 160323/583

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the username parameter under the Admin Panel. CVE ID : CVE-2023-	N/A	A-SIM-SIMP- 160323/584
, ,			24364		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the Description parameter under the Create ticket function. CVE ID : CVE-2023- 24652	N/A	A-SIM-SIMP- 160323/585
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the oldpass parameter under the Change Password function. CVE ID : CVE-2023- 24653	N/A	A-SIM-SIMP- 160323/586
Improper Neutralizat ion of Special Elements	27-Feb-2023	8.8	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL	N/A	A-SIM-SIMP- 160323/587

0-1

1-2

2-3

3-4 4-5 Page **324** of **859** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			injection vulnerability via the name parameter under the Request a Quote function.		
			CVE ID : CVE-2023- 24654		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL	27-Feb-2023	8.8	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the subject parameter under the Create Ticket function.	N/A	A-SIM-SIMP- 160323/588
Injection')			CVE ID : CVE-2023- 24656		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the name parameter on the registration page.	N/A	A-SIM-SIMP- 160323/589
Scripting J			CVE ID : CVE-2023- 24651		
	ple_food_orde	0.			
Product: sin	nple_food_ord	ering_sys	tem		
Improper			A vulnerability was		
Neutralizat ion of Input During Web Page Generation	18-Feb-2023	5.4	found in SourceCodester Simple Food Ordering System 1.0. It has been classified as problematic. This affects an unknown	N/A	A-SIM-SIMP- 160323/590

CVSS Scoring Scale 0-1 1-2

2-3

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			part of the file process_order.php. The manipulation of the argument order leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB- 221451.		
			CVE ID : CVE-2023- 0902		
Vendor: sim	ple_responsiv	e_tourisn	n_website_project		
	nple_responsiv		_ ·		
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	26-Feb-2023	6.1	A vulnerability, which was classified as problematic, was found in SourceCodester Simple Responsive Tourism Website 1.0. This affects an unknown part of the file /tourism/rate_revie w.php. The manipulation of the argument id with the input 1"> <script>alert(111 1)</script> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the	N/A	A-SIM-SIMP- 160323/591

0-1

1-2

2-33-44-5Page 326 of 859

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. The associated identifier of this vulnerability is VDB- 221799.		
			CVE ID : CVE-2023- 1041		
Vendor: sm	eup				
Product: er	р				
Affected Ver	sion(s): tokyo_v	76r1m220	406		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	27-Feb-2023	8.8	Sme.UP ERP TOKYO V6R1M220406 was discovered to contain an OS command injection vulnerability via calls made to the XMService component. CVE ID : CVE-2023- 26759	N/A	A-SME-ERP- 160323/592
Unrestricte d Upload of File with Dangerous Type	27-Feb-2023	8.8	Sme.UP ERP TOKYO V6R1M220406 was discovered to contain an arbitrary file upload vulnerability. CVE ID : CVE-2023- 26762	N/A	A-SME-ERP- 160323/593
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Feb-2023	7.5	Sme.UP TOKYO V6R1M220406 was discovered to contain an arbitrary file download vulnerabilty via the component /ResourceService. CVE ID : CVE-2023- 26758	N/A	A-SME-ERP- 160323/594

0-1

1-2

5-6

6-7 7-8 8-9

Cleartext Storage of Sensitive Informatio27-Feb-20237.5Sme.UP ERP TOKYO V6R1M220406 was discovered to contain an information disclosure vulnerability via the /debug endpoint. This vulnerability allows attackers to access cleartext credentials needed to authenticate to the AS400 system.N/AVendor: smg-webdesignVendor: smg-webdesignTroduct: shortcode_for_font_awesome WordPress plugin before 1.4.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post puring21-Feb-20235.4M/A	A-SME-ERP- 160323/595
Product: shortcode_for_font_awesomeAffected Version(s): * Up to (excluding) 1.4.1Affected Version(s): * Up to (excluding) 1.4.1ImproperImproperImproperNeutralizatInputImproper <td></td>	
Affected Version(s): * Up to (excluding) 1.4.1Affected Version(s): * Up to (excluding) 1.4.1ImproperImproperImproperNeutralization ofImputImput	
ImproperImproperImproperNeutralizatImprotentImprotentImputImprotentImprotent	
ImproperFont AwesomeNeutralizatKordPress pluginInputKordPress pluginbefore 1.4.1 does notvalidate and escapesome of its shortcodeattributes beforeoutputting themback in a page/post	
During21-Feb-20235.4where the shortcodeN/AWeb Page Generation ('Cross-site Scripting')is embedded, which 	A-SMG-SHOR- 160323/596
Vendor: snyk	
Product: kubernetes_monitor	
Affected Version(s): * Up to (excluding) 2.0.0	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentica tion	28-Feb-2023	5.3	This vulnerability in the Snyk Kubernetes Monitor can result in irrelevant data being posted to a Snyk Organization, which could in turn obfuscate other, relevant, security issues. It does not expose the user of the integration to any direct security risk and no user data can be leaked. To exploit the vulnerability the attacker does not need to be authenticated to Snyk but does need to know the target's Integration ID (which may or may not be the same as the Organization ID, although this is an unpredictable UUID in either case). CVE ID : CVE-2023- 1065	https://github .com/snyk/ku bernetes- monitor/pull/ 1275, https://github .com/snyk/ku bernetes- monitor/com mit/5b9a782 1680bbfb6c4a 900ab05d898 ce2b2cc157, https://snyk.i o/blog/api- auth-vuln- snyk- kubernetes- cve-2023- 1065/	A-SNY-KUBE- 160323/597
Vendor: Spi	-				
Product: sp	-	()):	22240		
Affected Ver	sion(s): * Up to	(excluding			
N/A	28-Feb-2023	9.8	SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because serialization is mishandled. The fixed versions are	https://git.spi p.net/spip/spi p/commit/5a edf49b89415a 4df3eb775eee 3801a2b4b88 266, https://git.spi	A-SPI-SPIP- 160323/598

0-1

1-2

2-33-44-5Page 329 of 859

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
			3.2.18, 4.0.10, 4.1.8, and 4.2.1. CVE ID : CVE-2023- 27372	p.net/spip/spi p/commit/96f beb38711c67 06e62457f2b 732a652a04a 409d						
Affected Ver	Affected Version(s): * Up to (including) 4.1.5									
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	9.8	SPIP v4.1.5 and earlier was discovered to contain a SQL injection vulnerability via the _oups parameter. This vulnerability allows attackers to execute arbitrary code via a crafted POST request. CVE ID : CVE-2023- 24258	N/A	A-SPI-SPIP- 160323/599					
Affected Ver	sion(s): 4.2.0			-						
N/A	28-Feb-2023	9.8	SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because serialization is mishandled. The fixed versions are 3.2.18, 4.0.10, 4.1.8, and 4.2.1. CVE ID : CVE-2023- 27372	https://git.spi p.net/spip/spi p/commit/5a edf49b89415a 4df3eb775eee 3801a2b4b88 266, https://git.spi p.net/spip/spi p/commit/96f beb38711c67 06e62457f2b 732a652a04a 409d	A-SPI-SPIP- 160323/600					
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.10										
N/A	28-Feb-2023	9.8	SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because	https://git.spi p.net/spip/spi p/commit/5a edf49b89415a 4df3eb775eee	A-SPI-SPIP- 160323/601					
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			serialization is mishandled. The fixed versions are 3.2.18, 4.0.10, 4.1.8, and 4.2.1. CVE ID : CVE-2023- 27372	3801a2b4b88 266, https://git.spi p.net/spip/spi p/commit/96f beb38711c67 06e62457f2b 732a652a04a 409d	
Affected Ver	sion(s): From (i	ncluding)	4.1.0 Up to (excluding)	4.1.8	
N/A	28-Feb-2023	9.8	SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because serialization is mishandled. The fixed versions are 3.2.18, 4.0.10, 4.1.8, and 4.2.1. CVE ID : CVE-2023- 27372	https://git.spi p.net/spip/spi p/commit/5a edf49b89415a 4df3eb775eee 3801a2b4b88 266, https://git.spi p.net/spip/spi p/commit/96f beb38711c67 06e62457f2b 732a652a04a 409d	A-SPI-SPIP- 160323/602
Vendor: ss-	proj				
Product: sh	irasagi				
Affected Ver	sion(s): * Up to	(including	g) 1.16.2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	24-Feb-2023	5.4	Stored cross-site scripting vulnerability in Schedule function of SHIRASAGI v1.16.2 and earlier versions allows a remote authenticated attacker to inject an arbitrary script. CVE ID : CVE-2023- 22425	https://www. ss- proj.org/supp ort/938.html	A-SSSHIR- 160323/603
Improper Neutralizat	24-Feb-2023	4.8	Stored cross-site scripting	https://www. ss-	A-SSSHIR- 160323/604

0-1

1-2

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			vulnerability in Theme switching function of SHIRASAGI v1.16.2 and earlier versions allows a remote attacker with an administrative privilege to inject an arbitrary script. CVE ID : CVE-2023- 22427	proj.org/supp ort/938.html	
Vendor: sta	gil			<u> </u>	
Product: sta	agil_navigation				
Affected Ver	sion(s): * Up to	(excluding			
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Feb-2023	7.5	An unauthenticated path traversal vulnerability affects the "STAGIL Navigation for Jira - Menu & Themes" plugin before 2.0.52 for Jira. By modifying the fileName parameter to the snjCustomDesignCon fig endpoint, it is possible to traverse and read the file system.	N/A	A-STA-STAG- 160323/605
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Feb-2023	7.5	CVE ID : CVE-2023- 26255 An unauthenticated path traversal vulnerability affects the "STAGIL Navigation for Jira - Menu & Themes" plugin before 2.0.52 for Jira. By modifying the fileName parameter to the	N/A	A-STA-STAG- 160323/606

0-1

1-2

2-3

3-4 4-5 Page **332** of **859** 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			snjFooterNavigation Config endpoint, it is possible to traverse and read the file system. CVE ID : CVE-2023- 26256		
Vendor: stra	ategy11				
Product: for	midable_form	_builder			
Affected Vers	sion(s): * Up to	(excluding	g) 5.5.7		
Cross-Site Request Forgery (CSRF)	28-Feb-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Strategy11 Form Builder Team Formidable Forms plugin <= 5.5.6 versions. CVE ID : CVE-2023- 24419	N/A	A-STR-FORM- 160323/607
Vendor: stru	uktur				1
Product: lib	heif				
Affected Vers	sion(s): 1.14.2			r	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Feb-2023	7.8	There is a vulnerability in the strided image data parsing code in the emscripten wrapper for libheif. An attacker could exploit this through a crafted image file to cause a buffer overflow in linear memory during a memcpy call.	https://github .com/struktur ag/libheif/pul l/759	A-STR-LIBH- 160323/608
,			CVE ID : CVE-2023- 0996		

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: su	do	I			
Affected Ver	sion(s): * Up to	(excludin	g) 1.9.13		
Double Free	28-Feb-2023	7.2	Sudo before 1.9.13p2 has a double free in the per-command chroot feature. CVE ID : CVE-2023- 27320	N/A	A-SUD-SUDO- 160323/609
Affected Ver	sion(s): 1.9.13				
Double Free	28-Feb-2023	7.2	Sudo before 1.9.13p2 has a double free in the per-command chroot feature. CVE ID : CVE-2023- 27320	N/A	A-SUD-SUDO- 160323/610
Vendor: Tea	ampass			•	
Product: tea	ampass				
Affected Ver	sion(s): * Up to	(excludin	g) 3.0.0.22		
External Control of File Name or Path	27-Feb-2023	7.1	External Control of File Name or Path in GitHub repository nilsteampassnet/tea mpass prior to 3.0.0.22. CVE ID : CVE-2023- 1070	https://huntr. dev/bounties/ 318bfdc4- 7782-4979- 956f- 9ba2cc44889cc , https://github .com/nilsteam passnet/team pass/commit/ 0af3574caba2 7a61b16dc25 c94fa51ae12d 2d967	A-TEA-TEAM- 160323/611
Vendor: tec	hpowerup			<u> </u>	<u> </u>
Product: dr	am_calculator_	for_ryzei	1		
Affected Ver	sion(s): 1.7.3				
Improper Initializatio n	26-Feb-2023	7.8	A vulnerability, which was classified as critical, has been	N/A	A-TEC-DRAM- 160323/612
		1 2			
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 334 of 859	-6 6-7 7-8	3 8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			found in TechPowerUp Ryzen DRAM Calculator 1.2.0.5. This issue affects some unknown processing in the library WinRing0x64.sys. The manipulation leads to improper initialization. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB- 221807. CVE ID : CVE-2023- 1048		
Product: rea	altemp				
Affected Ver	sion(s): 3.7.0.0				
Improper Initializatio n	26-Feb-2023	7.8	A vulnerability classified as critical was found in TechPowerUp RealTemp 3.7.0.0. This vulnerability affects unknown code in the library WinRing0x64.sys. The manipulation leads to improper initialization. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. VDB-221806 is the identifier	https://github .com/zeze- zeze/Window sKernelVuln/t ree/master/C VE-2023- 1047	A-TEC-REAL- 160323/613

0-1

1-2

2-33-44-5Page 335 of 859

8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. CVE ID : CVE-2023- 1047		
Vendor: tftr	d64_project				
Product: tft					
Affected Ver					
Unquoted Search Path or Element	17-Feb-2023	7.8	A vulnerability was found in phjounin TFTPD64-SE 4.64 and classified as critical. This issue affects some unknown processing of the file tftpd64_svc.exe. The manipulation leads to unquoted search path. An attack has to be approached locally. The associated identifier of this vulnerability is VDB-221351. CVE ID : CVE-2023-	N/A	A-TFT-TFTP- 160323/614
Vendor: the	mekraft		0887		
Product: bu					
	sion(s): * Up to	(excludin	g) 2.7.8		
Deserializa tion of Untrusted Data	23-Feb-2023	9.8	The BuddyForms WordPress plugin, in versions prior to 2.7.8, was affected by an unauthenticated insecure deserialization issue. An unauthenticated attacker could leverage this issue to call files using a PHAR wrapper that	N/A	A-THE-BUDD- 160323/615
		1 2		6 67 7	0 0 0 40
CVSS Scoring S	Scale 0-1	1-2 2	- 3 3-4 4-5 5 Page 336 of 859	-6 6-7 7-	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. CVE ID : CVE-2023-				
			26326				
Vendor: thi	-						
Product: thi							
Affected Vers	sion(s): 3.4.1						
Use of Hard- coded Credentials	23-Feb-2023	9.8	ThingsBoard 3.4.1 could allow a remote attacker to gain elevated privileges because hard-coded service credentials (usable for privilege escalation) are stored in an insecure format. (To read this stored data, the attacker needs access to the application server or its source code.) CVE ID : CVE-2023- 26462	N/A	A-THI-THIN- 160323/616		
Vendor: Tib	CO						
Product: bu	sinessconnect						
Affected Ver	sion(s): * Up to	(excluding	g) 7.3.1				
Improper Neutralizat ion of Input During Web Page Generation	22-Feb-2023	5.4	The BusinessConnect UI component of TIBCO Software Inc.'s TIBCO BusinessConnect contains easily exploitable Reflected	https://www. tibco.com/ser vices/support /advisories	A-TIB-BUSI- 160323/617		
CVSS Scoring S	CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						
			Page 337 of 859				

('Cross-site Scripting') Cross Site Scripting (XSS) vulnerabilities that allow a low privileged attacker with network access to execute scripts targeting the affected system or the victim's local system. Affected releases are TIBCO Software Inc's TIBCO BusinessConnect: versions 7.3.0 and below. CVE ID : CVE-2023- 26214 Vendor: timed_content_project Product: timed_content_project Product: timed_content_project Product: timed_content_project Product: timed_content Affected Version(s): * Up to (excluding) 2.73 Meutralizat ion of Input During Web Page Generation ('Cross-site Scripting') N/A 21-Feb-2023 5.4 5.4 See boord validate and escape outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. CVE ID : CVE-2023- 0067 N/A Vendor: tri	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Vendor: timed_content_projectProduct: timed_content_projectAffected Version(s): * Up to (excluding) 2.73Affected Version(s): * Up to (excluding) 2.73Improper Neutralization of Input During Web Page Generation ('Cross-site' Scripting')The Timed Content WordPress plugin before 2.73 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. CVE ID : CVE-2023- 067N/AA-TIM-TIME- 160323/618Vendor: triProduct: gigpressAffected Version(s): * Up to (including) 2.3.28	•			(XSS) vulnerabilities that allow a low privileged attacker with network access to execute scripts targeting the affected system or the victim's local system. Affected releases are TIBCO Software Inc.'s TIBCO BusinessConnect: versions 7.3.0 and below.						
Product: timed_contentAffected Version(s): * Up to (excluding) 2.73Improper Neutralizati ion of Input During Web Page Generation ('Cross-site) Scripting')The Timed Content WordPress plugin before 2.73 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.N/AA-TIM-TIME- 160323/618Vendor: triProduct: gigpressAffected Version(s): * Up to (including) 2.3.28										
Affected Version(s): * Up to (excluding) 2.73Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')The Timed Content WordPress plugin before 2.73 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. CVE ID : CVE-2023- 0667N/AA-TIM-TIME- 160323/618Vendor: triFeb-20125.4Feb-2012A-TIM-TIME- 160323/618Product: gigpressFeb-20125.4Feb-2012A-TIM-TIME- 160323/618Affected Version(s): * Up to (including) 2.3.28Feb-2012Feb-2012Feb-2012Affected Version(s): * Up to (including) 2.3.28Feb-2012Feb-2012Affected Version(s): * Up to (including) 2.3.28Feb-2012Feb-2012		-	oject							
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')21-Feb-20235.4The Timed Content WordPress plugin before 2.73 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.N/AA-TIM-TIME- 160323/618Vendor: triProduct: gigpressAffected Version(s): * Up to (including) 2.3.28			(avaludin	~) 2.72						
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')21-Feb-2023S.4WordPress plugin before 2.73 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.N/AA-TIM-TIME- 160323/618Vendor: triVendor: triVendor: triArriw IIII Provide and above to perform Stored Cross-Site Scripting attacks.CVE ID : CVE-2023- 0667Arriw IIII Provide IIIII Provide IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Affected ver	sion(s): [•] Op to	(excluding			1				
Product: gigpress Affected Version(s): * Up to (including) 2.3.28	Neutralizat ion of Input During Web Page Generation ('Cross-site	21-Feb-2023	5.4	WordPress plugin before 2.73 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. CVE ID : CVE-2023-	N/A					
Affected Version(s): * Up to (including) 2.3.28	Vendor: tri	Vendor: tri								
	Product: gigpress									
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Affected Ver	sion(s): * Up to	(including	g) 2.3.28						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	The GigPress WordPress plugin through 2.3.28 does not validate and escape some of its shortcode attributes before using them in SQL statement/s, which could allow any authenticated users, such as subscriber to perform SQL Injection attacks CVE ID : CVE-2023- 0381	N/A	A-TRI-GIGP- 160323/619
Vendor: tru	stedcomputing	ggroup			
	usted_platform	_module			
Affected Ver	sion(s): 2.0			1	
Out-of- bounds Write	28-Feb-2023	7.8	An out-of-bounds write vulnerability exists in TPM2.0's Module Library allowing writing of a 2-byte data past the end of TPM2.0 command in the CryptParameterDecr yption routine. An attacker who can successfully exploit this vulnerability can lead to denial of service (crashing the TPM chip/process or rendering it unusable) and/or arbitrary code execution in the TPM context. CVE ID : CVE-2023- 1017	https://truste dcomputinggr oup.org/wp- content/uploa ds/TCGVRT00 07-Advisory- FINAL.pdf, https://truste dcomputinggr oup.org/about /security/	A-TRU-TRUS- 160323/620

0-1

1-2

2-33-44-5Page 339 of 859

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Out-of- bounds Read	28-Feb-2023	5.5	An out-of-bounds read vulnerability exists in TPM2.0's Module Library allowing a 2-byte read past the end of a TPM2.0 command in the CryptParameterDecr yption routine. An attacker who can successfully exploit this vulnerability can read or access sensitive data stored in the TPM.	https://truste dcomputinggr oup.org/wp- content/uploa ds/TCGVRT00 07-Advisory- FINAL.pdf, https://truste dcomputinggr oup.org/about /security/	A-TRU-TRUS- 160323/621				
			CVE ID : CVE-2023- 1018						
Vendor: typ									
Product: typ	•								
Affected Ver	sion(s): * Up to	(excluding	g) 1.2.0						
N/A	22-Feb-2023	9.8	typecho 1.1/17.10.30 was discovered to contain a remote code execution (RCE) vulnerability via install.php.	N/A	A-TYP-TYPE- 160323/622				
			CVE ID : CVE-2023- 24114						
Vendor: ujc	ms								
Product: ujo	cms								
Affected Ver	Affected Version(s): From (including) 4.1.3 Up to (excluding) 5.5.1								
Improper Neutralizat ion of Input During Web Page Generation	17-Feb-2023	6.1	A cross-site scripting (XSS) vulnerability in UJCMS v4.1.3 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the URL	https://github .com/ujcms/u jcms/issues/3	A-UJC-UJCM- 160323/623				
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10				
	-		Page 340 of 859						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			parameter under the Add New Articles function.		
			CVE ID : CVE-2023- 24369		
Vendor: uptime-kuma_project					
Product: uptime-kuma					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	Uptime Kuma is a self-hosted monitoring tool. In versions prior to 1.20.0 the Uptime Kuma status page allows a persistent XSS attack. Users are advised to upgrade. There are no known workarounds for this vulnerability. CVE ID : CVE-2023- 25810	N/A	A-UPT-UPTI- 160323/624
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	Uptime Kuma is a self-hosted monitoring tool. In versions prior to 1.20.0 the Uptime Kuma `name` parameter allows a persistent XSS attack. Users are advised to upgrade. There are no known workarounds for this vulnerability. CVE ID : CVE-2023- 25811	N/A	A-UPT-UPTI- 160323/625
Vendor: utilities_project					
Product: utilities					
Affected Ver	sion(s): * Up to	(including	g) 1.0.6		

0-1

1-2

Page **341** of **859**

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improperly Controlled Modificatio n of Object Prototype Attributes ('Prototype Pollution')	28-Feb-2023	7.5	All versions of the package utilities are vulnerable to Prototype Pollution via the _mix function. CVE ID : CVE-2023- 26105	N/A	A-UTI-UTIL- 160323/626
Vendor: vek	ctor-inc				
Product: vk	_all_in_one_exp	pansion_l	ınit		
Affected Vers	sion(s): * Up to	(excluding	g) 9.86.0.0		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	The VK All in One Expansion Unit WordPress plugin before 9.86.0.0 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. CVE ID : CVE-2023- 0230	N/A	A-VEK-VK_A- 160323/627
Vendor: ver	sionn_project				
Product: ve	rsionn				
Affected Ver	sion(s): * Up to	(excludin	g) 1.1.0		
Improper Neutralizat ion of Special Elements used in a Command ('Comman	20-Feb-2023	9.8	versionn, software for changing version information across multiple files, has a command injection vulnerability in all versions prior to version 1.1.0. This	https://github .com/commen thol/versionn /commit/2ca 128823efe962 b37f2698f0eb 530c2b12484 2d	A-VER-VERS- 160323/628

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
d Injection')			issue is patched in version 1.1.0. CVE ID : CVE-2023-						
			25805						
Vendor: Vm	Vendor: Vmware								
	rbon_black_ap	-							
Affected Ver	sion(s): From (i	ncluding)	8.7.0 Up to (excluding)	8.7.8					
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	22-Feb-2023	7.2	VMware Carbon Black App Control 8.7.x prior to 8.7.8, 8.8.x prior to 8.8.6, and 8.9.x.prior to 8.9.4 contain an injection vulnerability. A malicious actor with privileged access to the App Control administration console may be able to use specially crafted input allowing access to the underlying server operating system. CVE ID : CVE-2023- 20858	https://www. vmware.com/ security/advis ories/VMSA- 2023- 0004.html	A-VMW-CARB- 160323/629				
Affected Ver	sion(s): From (i	ncluding)	8.8.0 Up to (excluding)	8.8.6					
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t	22-Feb-2023	7.2	VMware Carbon Black App Control 8.7.x prior to 8.7.8, 8.8.x prior to 8.8.6, and 8.9.x.prior to 8.9.4 contain an injection vulnerability. A malicious actor with privileged access to the App Control administration	https://www. vmware.com/ security/advis ories/VMSA- 2023- 0004.html	A-VMW-CARB- 160323/630				

0-1

1-2

2-3

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection') Affected Vers	<mark>sion(s): From (</mark> i	ncluding)	console may be able to use specially crafted input allowing access to the underlying server operating system. CVE ID : CVE-2023- 20858 8.9.0 Up to (excluding)	<mark>8.9.4</mark>	
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	22-Feb-2023	7.2	VMware Carbon Black App Control 8.7.x prior to 8.7.8, 8.8.x prior to 8.8.6, and 8.9.x.prior to 8.9.4 contain an injection vulnerability. A malicious actor with privileged access to the App Control administration console may be able to use specially crafted input allowing access to the underlying server operating system. CVE ID : CVE-2023- 20858	https://www. vmware.com/ security/advis ories/VMSA- 2023- 0004.html	A-VMW-CARB- 160323/631
Product: vro	ealize_automa	tion	L	I	L
Affected Ver	sion(s): From (i	ncluding)	8.0 Up to (excluding) 8.	.11.1	
Improper Restriction of XML External Entity Reference	22-Feb-2023	8.8	ZMware vRealizeOrchestratorOntains an XMLExternal Entity (XXE)Pulnerability. Analicious actor, withnon-administrativeoccess to vRealizeOrchestrator, may be		A-VMW-VREA- 160323/632
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	3 8-9 9-10

Page 344 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to use specially crafted input to bypass XML parsing restrictions leading to access to sensitive information or possible escalation of privileges. CVE ID : CVE-2023- 20855		
Product: vr	ealize_orchesti	rator		L	
Affected Ver	sion(s): From (i	ncluding)	8.0 Up to (excluding) 8.	11.1	
Improper Restriction of XML External Entity Reference	22-Feb-2023	8.8	VMware vRealize Orchestrator contains an XML External Entity (XXE) vulnerability. A malicious actor, with non-administrative access to vRealize Orchestrator, may be able to use specially crafted input to bypass XML parsing restrictions leading to access to sensitive information or possible escalation of privileges.	https://www. vmware.com/ security/advis ories/VMSA- 2023- 0005.html	A-VMW-VREA- 160323/633
			CVE ID : CVE-2023- 20855		
	orkspace_one_o				
Affected Ver	sion(s): * Up to	(excluding			
Missing Authentica tion for Critical Function	28-Feb-2023	6.8	VMware Workspace ONE Content contains a passcode bypass vulnerability. A malicious actor, with access to a users rooted device, may be able to	https://www. vmware.com/ security/advis ories/VMSA- 2023- 0006.html	A-VMW-WORK- 160323/634

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			bypass the VMware Workspace ONE Content passcode.					
			CVE ID : CVE-2023- 20857					
Vendor: vox2png_project								
Product: vo	x2png							
Affected Vers	sion(s): 1.0							
Heap- based Buffer Overflow	24-Feb-2023	5.5	A vulnerability classified as critical was found in vox2png 1.0. Affected by this vulnerability is an unknown functionality of the file vox2png.c. The manipulation leads to heap-based buffer overflow. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB- 221743. CVE ID : CVE-2023- 1010	https://github .com/10cksYi qiyinHangzho uTechnology/ vox2png/blob /main/READ ME.md	A-VOX-VOX2- 160323/635			
Vendor: wa	-							
Product: wa		(in clustic	2) E 0					
	sion(s): * Up to	Cinciuaing	5J 5.U					
Improper Neutralizat ion of Input During Web Page Generation	27-Feb-2023	5.4	WangEditor v5 was discovered to contain a cross-site scripting (XSS) vulnerability via the	N/A	A-WAN-WANG- 160323/636			
	Scale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			component /dist/index.js. CVE ID : CVE-2023- 24251		
Vendor: we	intek				
Product: ea	sybuilder_pro				
Affected Ver	sion(s): * Up to	(excluding	g) 6.07.02.480		-
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.8	The listed versions for Weintek EasyBuilder Pro are vulnerable to a ZipSlip attack caused by decompiling a malicious project file. This may allow an attacker to gain control of the user's computer or gain access to sensitive data. CVE ID : CVE-2023- 0104	N/A	A-WEI-EASY- 160323/637
Affected Ver	sion(s): From (i	ncluding)	6.08.01.190 Up to (excl	uding) 6.08.01.3	50
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.8	The listed versions for Weintek EasyBuilder Pro are vulnerable to a ZipSlip attack caused by decompiling a malicious project file. This may allow an attacker to gain control of the user's computer or gain access to sensitive data. CVE ID : CVE-2023- 0104	N/A	A-WEI-EASY- 160323/638
Vendor: wo	w-company				
Product: wp	o_coder				
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 347 of 859	<mark>-6 6-7 7-8</mark>	3 8-9 <mark>9-10</mark>

Page 347 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): * Up to	(including	g) 2.5.3		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	4.9	The WP Coder – add custom html, css and js code plugin for WordPress is vulnerable to time- based SQL Injection via the 'id' parameter in versions up to, and including, 2.5.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with administrative privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. CVE ID : CVE-2023- 0895	https://plugin s.trac.wordpre ss.org/change set?old=2757 782&old_path =wp- coder%2Ftru nk%2Fadmin %2Fpartials% 2Finclude- data.php&new =&new_path= wp- coder%2Ftru nk%2Fadmin %2Fpartials% 2Finclude- data.php	A-WOW-WP_C- 160323/639
Vendor: wp	devart				
Product: bo	oking_calenda	r			
Affected Ver	sion(s): * Up to	(excluding	g) 3.2.4		
Cross-Site Request Forgery (CSRF)	17-Feb-2023	5.4	Cross-Site Request Forgery (CSRF) vulnerability in WpDevArt Booking calendar, Appointment Booking System plugin <= 3.2.3	N/A	A-WPD-BOOK- 160323/640

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 348 of 859										

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			versions affects plugin forms actions (create, duplicate, edit, delete).				
			CVE ID : CVE-2023- 24388				
Product: or	ganization_cha	rt			1		
Affected Ver	sion(s): * Up to	(including	g) 1.4.4				
Cross-Site Request Forgery (CSRF)	e 23-Feb-2023 8.8 Forgery (CSRF) vulnerability in WpDevArt Organization chart <= 1.4.4 versions.		vulnerability in WpDevArt Organization chart	N/A	A-WPD-ORGA- 160323/641		
			CVE ID : CVE-2023- 24384				
Product: responsive_vertical_icon_menu							
Affected Ver	sion(s): * Up to	(excluding	g) 1.5.9				
Cross-Site Request Forgery (CSRF)	28-Feb-2023	5.4	Cross-Site Request Forgery (CSRF) vulnerability in wpdevart Responsive Vertical Icon Menu plugin <= 1.5.8 can lead to theme deletion. CVE ID : CVE-2023- 23983	N/A	A-WPD-RESP- 160323/642		
Vendor: wp	-						
Product: rev							
Affected Ver	sion(s): * Up to	(excluding					
Improper Neutralizat ion of Special Elements used in an SQL Command	23-Feb-2023	8.8	The 'rx_export_review' action in the ReviewX WordPress Plugin version < 1.6.4, is affected by an authenticated SQL injection	N/A	A-WPD-REVI- 160323/643		

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
('SQL Injection')			vulnerability in the 'filterValue' and 'selectedColumns' parameters.		
			CVE ID : CVE-2023- 26325		
Vendor: wp	geodirectory				
Product: ge	odirectory				
Affected Vers	sion(s): * Up to	(excluding	g) 2.2.24		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	7.2	The GeoDirectory WordPress plugin before 2.2.24 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin.	N/A	A-WPG-GEOD- 160323/644
Vendor: wn	_font_awesome	e project	CVE ID : CVE-2023- 0278		
•	_font_awesom	-1 >			
-	sion(s): * Up to		g) 1.7.9		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The WP Font Awesome WordPress plugin before 1.7.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embedded, which could allow users with the contributor role and above to perform Stored	N/A	A-WPWP_F- 160323/645
CVSS Scoring S	icale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-	8 8-9 9-10
		1 2	Page 350 of 859		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			Cross-Site Scripting attacks. CVE ID : CVE-2023- 0271				
Vendor: xos	slab						
Product: ea	sy_file_locker						
Affected Ver	sion(s): 2.2.0.18	34					
Improper Resource Shutdown or Release	18-Feb-2023	7.8	A vulnerability, which was classified as problematic, was found in Xoslab Easy File Locker 2.2.0.184. This affects the function MessageNotifyCallba ck in the library xlkfs.sys. The manipulation leads to denial of service. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-221457 was assigned to this vulnerability. CVE ID : CVE-2023- 0908	N/A	A-XOS-EASY- 160323/646		
	ga_class_registi	-					
	ga_class_regist	ration_sy	vstem				
Affected Ver	sion(s): 1.0		A surla oscibilita				
Improper Neutralizat ion of Special Elements used in an SQL	23-Feb-2023	9.8	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0 and classified as critical. This issue affects	N/A	A-YOG-YOGA- 160323/647		
SQL Ims issue arects 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 ('SQL Injection')			some unknown processing of the file admin/registrations /update_status.php of the component Status Update Handler. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB- 221675. CVE ID : CVE-2023- 0980		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	23-Feb-2023	9.8	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0. It has been classified as critical. Affected is an unknown function of the component Delete User. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB- 221676.	N/A	A-YOG-YOGA- 160323/648
Improper			CVE ID : CVE-2023- 0981 A vulnerability was		
Neutralizat ion of Special Elements	23-Feb-2023	9.8	found in SourceCodester Yoga Class Registration System 1.0. It has	N/A	A-YOG-YOGA- 160323/649

0-1

1-2

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
used in an SQL Command ('SQL Injection')			been declared as critical. Affected by this vulnerability is an unknown functionality of the component Add Class Entry. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The identifier VDB- 221677 was assigned to this vulnerability. CVE ID : CVE-2023- 0982			
Vendor: zet	acomponenets	;	0702			
Product: my	vctools					
Affected Ver	sion(s): 2008-0	9-23				
N/A	22-Feb-2023	9.8	MvcTools 6d48cd6830fc1df1d 8c9d61caa1805fd6a 1b7737 was discovered to contain a code execution backdoor via the request package (requirements.txt). This vulnerability allows attackers to access sensitive user information and execute arbitrary code. CVE ID : CVE-2023-	N/A	A-ZET-MVCT- 160323/650	
Vendor: Zor	neminder		24108			
Product: Zoneminder						

0-1

1-2

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): * Up to (excluding) 1.36.33							
Missing Authorizati on	25-Feb-2023	9.8	ZoneMinder is a free, open source Closed- circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 are vulnerable to Unauthenticated Remote Code Execution via Missing Authorization. There are no permissions check on the snapshot action, which expects an id to fetch an existing monitor but can be passed an object to create a new one instead. TriggerOn ends up calling shell_exec using the supplied Id. This issue is fixed in This issue is fixed in This issue is fixed in Versions 1.36.33 and 1.37.33. CVE ID : CVE-2023- 26035	https://github .com/ZoneMin der/zonemind er/security/a dvisories/GHS A-72rg-h4vf- 29gr	A-ZON-ZONE- 160323/651		
Untrusted Search Path	25-Feb-2023	9.8	ZoneMinder is a free, open source Closed- circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33	https://github .com/ZoneMin der/zonemind er/security/a dvisories/GHS A-h5m9-6jjc- cgmw	A-ZON-ZONE- 160323/652		

0-1

1-2

2-3 3-4 4-5 Page 354 of 859 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a Local File Inclusion (Untrusted Search Path) vulnerability via /web/index.php. By controlling \$view, any local file ending in .php can be executed. This is supposed to be mitigated by calling detaintPath, however dentaintPath does not properly sandbox the path. This can be exploited by constructing paths like "/./", which get replaced by "/". This issue is patched in versions 1.36.33 and 1.37.33. CVE ID : CVE-2023- 26036		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	9.8	ZoneMinder is a free, open source Closed- circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain an SQL Injection. The minTime and maxTime request parameters are not properly validated and could be used execute arbitrary SQL. This issue is	https://github .com/ZoneMin der/zonemind er/security/a dvisories/GHS A-65jp-2hj3- 3733	A-ZON-ZONE- 160323/653

0-1

1-2

2-33-44-5Page 355 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in versions 1.36.33 and 1.37.33. CVE ID : CVE-2023- 26037		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	8.8	ZoneMinder is a free, open source Closed- circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 are affected by a SQL Injection vulnerability. The (blind) SQL Injection vulnerability is present within the 'filter[Query][terms] [0][attr]` query string parameter of the `/zm/index.php` endpoint. A user with the View or Edit permissions of Events may execute arbitrary SQL. The resulting impact can include unauthorized data access (and modification), authentication and/or authorization bypass, and remote code execution. CVE ID : CVE-2023- 26034	https://github .com/ZoneMin der/zonemind er/security/a dvisories/GHS A-222j-wh8m- xjrx	A-ZON-ZONE- 160323/654
Improper Neutralizat ion of Special Elements	25-Feb-2023	8.8	ZoneMinder is a free, open source Closed- circuit television software application for Linux which	https://github .com/ZoneMin der/zonemind er/security/a dvisories/GHS	A-ZON-ZONE- 160323/655

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain an OS Command Injection via daemonControl() in (/web/api/app/Cont roller/HostControlle r.php). Any authenticated user can construct an api command to execute any shell command as the web user. This issue is patched in versions 1.36.33 and 1.37.33. CVE ID : CVE-2023- 26039	A-44q8-h2pw- cc9g	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	8.1	ZoneMinder is a free, open source Closed- circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain SQL Injection via malicious jason web token. The Username field of the JWT token was trusted when performing an SQL query to load the user. If an attacker could determine the HASH key used by ZoneMinder, they could generate a	https://github .com/ZoneMin der/zonemind er/security/a dvisories/GHS A-6c72- q9mw-mwx9	A-ZON-ZONE- 160323/656

0-1

1-2

2-33-44-5Page 357 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious JWT token and use it to execute arbitrary SQL. This issue is fixed in versions 1.36.33 and 1.37.33.		
			CVE ID : CVE-2023- 26032		
Untrusted Search Path	25-Feb-2023	6.5	ZoneMinder is a free, open source Closed- circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain a Local File Inclusion (Untrusted Search Path) vulnerability via web/ajax/modal.php , where an arbitrary php file path can be passed in the request and loaded. This issue is patched in versions 1.36.33 and 1.37.33. CVE ID : CVE-2023-	https://github .com/ZoneMin der/zonemind er/security/a dvisories/GHS A-wrx3-r8c4- r24w	A-ZON-ZONE- 160323/657
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	25-Feb-2023	6.1	26038 ZoneMinder is a free, open source Closed- circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 are vulnerable to Cross- site Scripting. Log entries can be	https://github .com/ZoneMin der/zonemind er/commit/57 bf25d39f12d6 20693f26068 b8441b4f3f0b 6c0, https://github .com/ZoneMin der/zonemind er/security/a	A-ZON-ZONE- 160323/658

0-1

1-2

2-3

3-4 4-5 Page **358** of **859** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injected into the database logs, containing a malicious referrer field. This is unescaped when viewing the logs in the web ui. This issue is patched in version 1.36.33.	dvisories/GHS A-68vf-g4qm- jr6v	
			CVE ID : CVE-2023- 25825		
Affected Ver	sion(s): From (i	ncluding)	1.37.0 Up to (excluding) 1.37.33	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	25-Feb-2023	6.1	ZoneMinder is a free, open source Closed- circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 are vulnerable to Cross- site Scripting. Log entries can be injected into the database logs, containing a malicious referrer field. This is unescaped when viewing the logs in the web ui. This issue is patched in version 1.36.33. CVE ID : CVE-2023- 25825	https://github .com/ZoneMin der/zonemind er/commit/57 bf25d39f12d6 20693f26068 b8441b4f3f0b 6c0, https://github .com/ZoneMin der/zonemind er/security/a dvisories/GHS A-68vf-g4qm- jr6v	A-ZON-ZONE- 160323/659
Affected Ver	sion(s): From (i	ncluding)	1.37.00 Up to (excludin	g) 1.37.33	
Missing Authorizati on	25-Feb-2023	9.8	ZoneMinder is a free, open source Closed- circuit television software application	https://github .com/ZoneMin der/zonemind er/security/a	A-ZON-ZONE- 160323/660

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 are vulnerable to Unauthenticated Remote Code Execution via Missing Authorization. There are no permissions check on the snapshot action, which expects an id to fetch an existing monitor but can be passed an object to create a new one instead. TriggerOn ends up calling shell_exec using the supplied Id. This issue is fixed in This issue is fixed in This issue is fixed in versions 1.36.33 and 1.37.33. CVE ID : CVE-2023- 26035	dvisories/GHS A-72rg-h4vf- 29gr	
Untrusted Search Path	25-Feb-2023	9.8	ZoneMinder is a free, open source Closed- circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain a Local File Inclusion (Untrusted Search Path) vulnerability via /web/index.php. By	https://github .com/ZoneMin der/zonemind er/security/a dvisories/GHS A-h5m9-6jjc- cgmw	A-ZON-ZONE- 160323/661

0-1

1-2

2-3 3-4 4-5 Page 360 of 859 5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controlling \$view, any local file ending in .php can be executed. This is supposed to be mitigated by calling detaintPath, however dentaintPath does not properly sandbox the path. This can be exploited by constructing paths like "/./", which get replaced by "/". This issue is patched in versions 1.36.33 and 1.37.33.		
			CVE ID : CVE-2023- 26036		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	9.8	ZoneMinder is a free, open source Closed- circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain an SQL Injection. The minTime and maxTime request parameters are not properly validated and could be used execute arbitrary SQL. This issue is fixed in versions 1.36.33 and 1.37.33. CVE ID : CVE-2023- 26037	https://github .com/ZoneMin der/zonemind er/security/a dvisories/GHS A-65jp-2hj3- 3733	A-ZON-ZONE- 160323/662

0-1

1-2

2-3

3-4 4-5 Page **361** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	8.8	ZoneMinder is a free, open source Closed- circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 are affected by a SQL Injection vulnerability. The (blind) SQL Injection vulnerability is present within the `filter[Query][terms] [0][attr]` query string parameter of the `/zm/index.php` endpoint. A user with the View or Edit permissions of Events may execute arbitrary SQL. The resulting impact can include unauthorized data access (and modification), authentication and/or authorization bypass, and remote code execution. CVE ID : CVE-2023- 26034	https://github .com/ZoneMin der/zonemind er/security/a dvisories/GHS A-222j-wh8m- xjrx	A-ZON-ZONE- 160323/663
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	25-Feb-2023	8.8	ZoneMinder is a free, open source Closed- circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33	https://github .com/ZoneMin der/zonemind er/security/a dvisories/GHS A-44q8-h2pw- cc9g	A-ZON-ZONE- 160323/664

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			contain an OS Command Injection via daemonControl() in (/web/api/app/Cont roller/HostControlle r.php). Any authenticated user can construct an api command to execute any shell command as the web user. This issue is patched in versions 1.36.33 and 1.37.33.		
			CVE ID : CVE-2023- 26039		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	8.1	ZoneMinder is a free, open source Closed- circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain SQL Injection via malicious jason web token. The Username field of the JWT token was trusted when performing an SQL query to load the user. If an attacker could determine the HASH key used by ZoneMinder, they could generate a malicious JWT token and use it to execute arbitrary SQL. This issue is fixed in	https://github .com/ZoneMin der/zonemind er/security/a dvisories/GHS A-6c72- q9mw-mwx9	A-ZON-ZONE- 160323/665

0-1

1-2

2-33-44-5Page 363 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 1.36.33 and 1.37.33.		
			CVE ID : CVE-2023- 26032		
Untrusted Search Path	25-Feb-2023	6.5	ZoneMinder is a free, open source Closed- circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain a Local File Inclusion (Untrusted Search Path) vulnerability via web/ajax/modal.php , where an arbitrary php file path can be passed in the request and loaded. This issue is patched in versions 1.36.33 and 1.37.33. CVE ID : CVE-2023- 26038	https://github .com/ZoneMin der/zonemind er/security/a dvisories/GHS A-wrx3-r8c4- r24w	A-ZON-ZONE- 160323/666
			Hardware		
Vendor: abu	15				
Product: tvi	ip_20000-2115	0			
Affected Ver	sion(s): -				
N/A	27-Feb-2023	7.2	ABUS TVIP 20000- 21150 devices allows remote attackers to execute arbitrary code via shell metacharacters in the /cgi- bin/mft/wireless_mf t ap field.	N/A	H-ABU-TVIP- 160323/667

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 26609		
Vendor: Axi	S				
Product: 20	7w				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	6.1	** UNSUPPORTED WHEN ASSIGNED ** A Vulnerability was discovered in Axis 207W network camera. There is a reflected XSS vulnerability in the web administration portal, which allows an attacker to execute arbitrary JavaScript via URL. CVE ID : CVE-2023- 22984	N/A	H-AXI-207W- 160323/668
Vendor: Cis					
Product: fir	epower_4100				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-FIRE- 160323/669

0-1

1-2

6-7

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges.		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	20015 A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-FIRE- 160323/670

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Product: fir	epower_4110				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-FIRE- 160323/671
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10

Page 367 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm-	H-CIS-FIRE- 160323/672

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016	bkpsky- H8FCQgsA				
	Product: firepower_4112							
Affected Vers	sion(s): -							

0-1

1-2

2-3

3-4 4-5 Page **369** of **859** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges.	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-FIRE- 160323/673

0-1

1-2

2-3

3-4 4-5 Page **370** of **859** 5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-FIRE- 160323/674

0-1

1-2

2-3

3-4 4-5 Page **371** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and other credentials. CVE ID : CVE-2023- 20016		
Product: fir	epower_4115	<u> </u>		L	
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-FIRE- 160323/675

0-1

1-2

2-3

3-4 4-5 Page **372** of **859** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges.		
			CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-FIRE- 160323/676

0-1

1-2

2-3

3-4 4-5 Page **373** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Product: fir	epower_4120				
Affected Ver	- sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-FIRE- 160323/677

0-1

1-2

2-3

3-4 4-5 Page **374** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-FIRE- 160323/678

0-1

1-2

2-3

3-4 4-5 Page **375** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023-					
			20016					
Product: firepower_4125								
Affected Ver	sion(s): -		A mula anability in the					
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-FIRE- 160323/679			

0-1

1-2

2-3

3-4 4-5 Page **376** of **859** 5-6

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-FIRE- 160323/680

0-1

1-2

2-3

3-4 4-5 Page **377** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
	epower_4140				
Affected Vers Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	sion(s): - 23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-FIRE- 160323/681

0-1

1-2

2-3

3-4 4-5 Page **378** of **859** 6-7

7-8

5-6

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-FIRE- 160323/682

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<pre>to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials.</pre>		
Product: fir	epower_4145				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity	H-CIS-FIRE- 160323/683
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10

Page 380 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges.	Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	
Use of Insufficient	23-Feb-2023	6.5	20015 A vulnerability in the backup configuration	https://sec.clo udapps.cisco.c	H-CIS-FIRE- 160323/684

0-1

1-2

2-33-44-5Page 381 of 859

5-6

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random			feature of Cisco UCS	om/security/c	
Values			Manager Software	enter/content	
			and in the	/CiscoSecurity	
			configuration export	Advisory/cisc	
			feature of Cisco FXOS	o-sa-ucsm-	
			Software could allow	bkpsky-	
			an unauthenticated	H8FCQgsA	
			attacker with access		
			to a backup file to		
			decrypt sensitive		
			information stored in		
			the full state and		
			configuration backup		
			files. This		
			vulnerability is due		
			to a weakness in the		
			encryption method		
			used for the backup		
			function. An attacker		
			could exploit this		
			vulnerability by		
			leveraging a static		
			key used for the		
			backup configuration		
			feature. A successful		
			exploit could allow		
			the attacker to		
			decrypt sensitive		
			information that is		
			stored in full state		
			and configuration		
			backup files, such as		
			local user		
			credentials,		
			authentication		
			server passwords,		
			Simple Network		
			Management		
			Protocol (SNMP)		
			community names,		
			and other		
			credentials.		

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20016		
Product: fir	epower_4150				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-FIRE- 160323/685

0-1

1-2

2-3

3-4 4-5 Page **383** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges.		
			CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-FIRE- 160323/686

0-1

1-2

2-3

3-4 4-5 Page **384** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Product: fir	epower_9300_	sm-24	20010		
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-FIRE- 160323/687

0-1

1-2

2-3

3-4 4-5 Page **385** of **859** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-FIRE- 160323/688

0-1

1-2

2-3

3-4 4-5 Page **386** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023-		
Product: fir	epower_9300_	sm-36	20016		
Affected Ver					
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-FIRE- 160323/689

0-1

1-2

2-3

3-4 4-5 Page **387** of **859** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-FIRE- 160323/690

0-1

1-2

2-3 3-4 4-5 Page 388 of 859 6-7

7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-FIRE- 160323/692

0-1

1-2

2-3

6-7 7-8

5-6

Product: firepower_9300_sm-44 A vulnerability in the cliss conserved to the con	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Product: firepower_9300_sm-44Affected Version(s): -Improper Neutralizat ion of Special Elements used in an OSA vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200,https://sec.clo udapps.cisco.c om/security/c (CiscoSecurity H-CIS-FIRE- 160323/693				<pre>the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials.</pre>				
Improper Neutralizat ion of SpecialA vulnerability in the CLI of Ciscohttps://sec.clo udapps.cisco.cH-CIS-FIRE- 160323/693Special Elements used in an OS23-Feb-20236.76.7Series, Ciscoenter/content Firepower 9300H-CIS-FIRE- 160323/693OS00Security Appliances, and Cisco UCS 6200,Advisory/cisc o-sa-nxfp-H-CIS-FIRE- 160323/693	Product: fir	epower_9300_	sm-44			<u> </u>		
Neutralizat ion of Special23-Feb-2023CLI of Cisco Firepower 4100udapps.cisco.c om/security/c enter/contentH-CIS-FIRE- 160323/693Elements used in an OS23-Feb-20236.7Series, Cisco Firepower 9300enter/content /CiscoSecurity Advisory/cisc and Cisco UCS 6200,H-CIS-FIRE- 160323/693	Affected Ver	sion(s): -						
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Neutralizat ion of Special Elements used in an	23-Feb-2023	6.7	CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances,	udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc			
	CVSS Scoring S	CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						

Page **391** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015	cmdinj- XXBZjtR	
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software	https://sec.clo udapps.cisco.c om/security/c enter/content	H-CIS-FIRE- 160323/694

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			and in the	/CiscoSecurity				
			configuration export	Advisory/cisc				
			feature of Cisco FXOS	o-sa-ucsm-				
			Software could allow	bkpsky-				
			an unauthenticated	H8FCQgsA				
			attacker with access					
			to a backup file to					
			decrypt sensitive					
			information stored in					
			the full state and					
			configuration backup					
			files. This					
			vulnerability is due					
			to a weakness in the					
			encryption method					
			used for the backup					
			function. An attacker					
			could exploit this					
			vulnerability by					
			leveraging a static					
			key used for the					
			backup configuration					
			feature. A successful					
			exploit could allow					
			the attacker to					
			decrypt sensitive					
			information that is					
			stored in full state					
			and configuration					
			backup files, such as					
			local user					
			credentials,					
			authentication					
			server passwords,					
			Simple Network					
			Management					
			Protocol (SNMP)					
			community names,					
			and other					
			credentials.					
			CVE ID : CVE-2023-					
			20016					
Product: fir	epower_9300_	sm-44_x_	3					
	Product: firepower_9300_sm-44_x_3							

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): -	L			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-FIRE- 160323/695

0-1

1-2

2-3 3-4 4-5 Page **394** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-FIRE- 160323/696

0-1

1-2

2-33-44-5Page 395 of 859

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Protocol (SNMP) community names, and other credentials.		
			CVE ID : CVE-2023- 20016		
Product: fir	epower_9300_	sm-48	L		
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-FIRE- 160323/697

0-1

1-2

2-3

3-4 4-5 Page **396** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-FIRE- 160323/698

0-1

1-2

2-3

3-4 4-5 Page **397** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Product: fir	epower_9300_	sm-56			
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-FIRE- 160323/699

0-1

1-2

2-3

3-4 4-5 Page **398** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-FIRE- 160323/700

0-1

1-2

2-3

3-4 4-5 Page **399** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Product: fir	epower_9300_	sm-56_x_	3		
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-FIRE- 160323/701

0-1

1-2

2-3

3-4 4-5 Page **400** of **859** 5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges.		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	20015 A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-FIRE- 160323/702

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Product: mo	ls_9000			L	
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/703
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10

Page **402** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: m					
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/704

0-1

1-2

2-3

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: mo	ds_9132t				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/705

0-1

1-2

2-3

3-4 4-5 Page **404** of **859** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023-		
			20050		
Product: me					
Affected Ver	sion(s): -		A vulnerability in the		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/706

0-1

1-2

2-3

3-4 4-5 Page **405** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: m	ds_9140				
Affected Ver	rsion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023 ds_9148	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/707

0-1

1-2

2-3

3-4 4-5 Page **406** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Ver	Affected Version(s): -								
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/708				
Product: mo									
Affected Ver	sion(s): -								
Improper Neutralizat ion of Special Elements	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity	H-CIS-MDS 160323/709				

1-2

5-6

6-7

3-4 4-5 5-6 2-3 Page 408 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: mo	ds_9200				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/711

0-1

1-2

2-3

3-4 4-5 Page **409** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: m	ds_9216				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/712

0-1

1-2

2-3

3-4 4-5 Page **410** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.		
			CVE ID : CVE-2023- 20050		
Product: m	ds_9216a				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/713

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20050		
Product: m	ds_9216i				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/714
Product: m	ds_9222i				
Affected Ver	sion(s): -				

0-1

1-2

2-3

3-4 4-5 Page **412** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/715
Product: mo					
Improper Neutralizat ion of Special Elements used in an OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli-	H-CIS-MDS 160323/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	cmdinject- euQVK9u	
Product: mo	ls_9396s				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/717

0-1

1-2

2-3

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023-		
			20050		
Product: mo					
Affected Ver Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	sion(s): - 23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/718

0-1

1-2

2-3 3-4 4-5 Page **415** of **859** 6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: m	ds_9500				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/719

0-1

1-2

2-3

3-4 4-5 Page **416** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: mo	ds_9506				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/720

0-1

1-2

2-3

3-4 4-5 Page **417** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Product: mo	ls_9509	I	L	L	L		
Affected Vers	sion(s): -						
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/721		
Affected Version(s): -							
Improper Neutralizat ion of Special	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated,	https://sec.clo udapps.cisco.c om/security/c enter/content	H-CIS-MDS 160323/722		
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 418 of 859	-6 6-7 7-8	8 8-9 9-10		

3-4 4-5 2-3 Page **418** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Elements used in an OS Command ('OS Command Injection')			local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	/CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u		
Product: mo	ls_9700					
Affected Vers	sion(s): -					
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/723	
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')			to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: mo	ds_9706			I	
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/724

0-1

1-2

2-3

3-4 4-5 Page **420** of **859** 8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: mo	ds 9710		20050		
Affected Ver					
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/725

0-1

1-2

2-3

3-4 4-5 Page **421** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: me					
Affected Ver Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-MDS 160323/726

0-1

1-2

2-33-44-5Page 422 of 859

6-7 7-8

5-6

Improper Improper Special Elements used in user.A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability by including crafted inguent of an affected command. An OS Command injection)Arsenance secute arbitrary commands on the underlying operating system of an affected device. This vulnerability by including crafted input as the affected command. An affected command. An affected command. An expective to insufficient vulnerability by including crafted input as the successful exploit could allow the underlying operating system of an affected device. This vulnerability by including crafted input as the affected command. An affected command. An successful exploit could allow the underlying operating system of an affected command. An affected command. An successful exploit could allow the underlying operating operating system or the underlying operating system of an affected command. An successful exploit could allow the poperating system operating system or the underlying operating system operating systemH-CIS-NEXU- to assert operation operating system or sanos-cli- mdinect- euQVK9uInstruct to the underlying operating system operating system operating system operating system operating system operating system operating system operating system operating syste	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an (OS Command Injection)7.8A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could execute arbitrary commands. An attacker could exploit this vulnerability by including crafted including crafted input as the argument of an affected command. A successful exploit this or san tacker to execute argument of an affected command. A successful exploit mis could allow the attacker to execute argument of an affected command. A successful exploit mis on the underlying operating system or the underlying operating system or the underlying operating system or the underlying operating system or the underlying operating systemIH-CIS-NEXU- it Advisory/cis or sa-nxos-cli- cmdinject- euQVK9uII-CIS-NEXU- it CVE ID : CVE-2023-CVE ID : CVE-2023-IH-CIS-NEXU- it CVE ID : CVE-2023-						
Affected Version(s): -Affected Version(s): -A Avulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands. An extacker could exploit this vulnerability by including crafted input as the attacker to execute arbitrary commands. An successful exploit could allow the attacker to execute arbitrary commands. A successful exploit could allow the attacker to execute arbitrary commands. A s						
Improper Neutralizat ion of Special Elements used in an (OS Command Injection')23-Feb-20237.8A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are ipassed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.Https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity/c enter/content /CiscoSecurity/c enter/content /CiscoSecurity endividence endividence could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.Https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity/c enter/content /CiscoSecurity/c enter/content /CiscoSecurity/c enter/content /CiscoSecurity/c enter/content /CiscoSecurity/c enter/content /CiscoSecurity/c enter/content /CiscoSecurity/c enter/content /CiscoSecurity/c enter/content /CiscoSecurity/c enter/content /CiscoSecurity/c enter/content /CiscoSecurity/c enter/content /CiscoSecurity/c enter/content /CiscoSecurity/c enter/content /CiscoSecurity/c enter/ciscoSecurity/c enter/ciscoSecurity/c enter/ciscoSecurity/c e	Product: ne	xus_1000v				
Improper Neutralizati ion of Special Elements used in an discontrandiction of Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. As successful exploit could allow the attacker to execute argument of an affected command. As successful exploit comdands on the underlying operating system with the privileges of the currently logged- in user.https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity enter/content <b< td=""><td>Affected Ver</td><td>sion(s): -</td><td></td><td></td><td></td><td></td></b<>	Affected Ver	sion(s): -				
Product: nexus_1000_virtual_edge	Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')			CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023-	udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject-	

0-1

1-2

2-3

3-4 4-5 Page **423** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Version(s): -								
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/728			
	Product: nexus_3016							
Affected Ver Improper Neutralizat ion of Special Elements	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity	H-CIS-NEXU- 160323/729			

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	
Product: ne	-				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/730
CVSS Scoring S	Scale 0-1	1-2 2		<mark>-6 6-7 7-</mark> 8	<u>8 8-9 9-10</u>
Page 425 of 859					

Page **425** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_3048				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/731

0-1

1-2

2-3

3-4 4-5 Page **426** of **859** 6-7

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	exus_3064				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/732

0-1

1-2

2-3

3-4 4-5 Page **427** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.		
			CVE ID : CVE-2023- 20050		
Product: ne	xus_3064-32t				
Affected Ver	sion(s): -				_
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/733

0-1

1-2

2-3

6-7 7-8

5-6

		CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20050		
Product: ne	xus_3064-t				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/734
Product: ne	xus_3064-x				
Affected Vers	sion(s): -				

0-1

1-2

2-3

3-4 4-5 Page **429** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/735		
Product: ne Affected Ver							
Improper Neutralizat ion of Special Elements used in an OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli-	H-CIS-NEXU- 160323/736		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10							

Page **430** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	cmdinject- euQVK9u	
Product: ne	xus_3064x				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/737

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023-		
			20050		
Product: ne					
Affected Ver Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	sion(s): - 23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/738

0-1

1-2

2-33-44-5Page 432 of 859

7-8

6-7

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_3100-v				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/739

0-1

1-2

2-3

3-4 4-5 Page **433** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_3100-z				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/740

0-1

1-2

2-3

3-4 4-5 Page **434** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Product: ne	xus_3100v	I	L	L	L		
Affected Vers	sion(s): -						
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/741		
	Product: nexus_31108pc-v Affected Version(s): -						
Improper Neutralizat ion of Special	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated,	https://sec.clo udapps.cisco.c om/security/c enter/content	H-CIS-NEXU- 160323/742		
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 435 of 859	-6 6-7 7-8	<u>8 8-9 9-10</u>		

Page 435 of 859

Elementslocal attacker to/CiscoSecurityused in anexecute arbitraryAdvisory/ciscOScommands on theo-sa-nxos-cli-Commandunderlying operatingcmdinject-('OSsystem of an affectedeuQVK9uCommanddevice. This	
Injection') vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023-	
20050 Product: nexus_31108pv-v	
Affected Version(s): -	
Improper Neutralizat ion of Special Elements Used in an OSA vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is duehttps://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9uH-CIS-NEXI 160323/74	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 Page 436 of 859	9-10

Page 436 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_31108tc-v	,	<u> </u>		<u> </u>
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/744

0-1

1-2

2-3

3-4 4-5 Page **437** of **859** 5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_31128pq		20030		
Affected Ver					
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/745

0-1

1-2

2-3

3-4 4-5 Page **438** of **859** 8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	exus_3132c-z				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/746

0-1

1-2

2-33-44-5Page 439 of 859

6-7 7-8

5-6

9-10

Image: Product: new: 3132qthe currently logged- in user. CVE D: CVE-2023- 20050Image: 20050Product: new: 3132qAffected Ver: 10: CVE-2023- 20050Affected Ver: 10: 10: CVE-2023- 20050Image: 10: 10: 10: 10: 10: 10: 10: 10: 10: 10	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an Injection')Z3-Feb-20237.8A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient vulnerability by including crafted input as the argument of an affected commands. An affected commands. An attacker could execute arbitrary commands on the underlying operating system of an affected device. This vulnerability by including crafted input as the argument of an affected commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected commands. An attacker to execute argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of not the underlying operating system with the privileges of argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of in user.H-CIS-NEXU- to in user.						
Affected Version(s): -Affected Version(s): -A Article of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands. An successful exploit could allow the attacker to execute argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands. An underlying operating system with the privileges of in user.H-CIS-NEXU- H-CIS-NEXU- 160323/747						
Improper Neutralizat ion of Special Elements used in an (OS Command Injection')23-Feb-20237.8A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity enter/content /CiscoSecurity/c enter/ciscoSecurity/c enter/ciscoSecurity/c enter/ciscoSecuri	Product: ne	xus_3132q				
Improper Neutralizat ion of Special Elements used in an 0/S23-Feb-20237.8CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. As successful exploit could allow the attacker to execute argument of an affected commands. An exploit this vulnerability by including crafted input as the argument of an affected command. As successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc euQVK9uH-CIS-NEXU- 160323/747	Affected Vers	sion(s): -				
Product: nexus_3132q-v	Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')		7.8	CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023-	udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject-	

0-1

1-2

2-3

3-4 4-5 Page **440** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Ver	Affected Version(s): -								
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/748				
	xus_3132q-x								
Affected Ver Improper Neutralizat ion of Special Elements	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity	H-CIS-NEXU- 160323/749				

CVSS Scoring Scale0-11-22-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	
Product: nexu	us_3132q-xl				
Affected Versio	on(s): -				
Improper Neutralizat ion of Special Elements used in an 2 OS Command ('OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject-	H-CIS-NEXU- 160323/750
Command Injection')			vulnerability is due to insufficient	euQVK9u	

Page **442** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_3132q-x\/	/3132q-x	l		
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/751

0-1

1-2

2-3

3-4 4-5 Page **443** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_3164q				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/752

0-1

1-2

2-3

3-4 4-5 Page **444** of **859** 6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.		
			CVE ID : CVE-2023- 20050		
Product: ne					
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/753

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20050		
Product: ne	xus_3172pq				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/754
	xus_3172pq-xl				
Affected Ver	sion(s): -				

0-1

1-2

2-3

3-4 4-5 Page **446** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/755				
	Product: nexus_3172pq\/pq-xl Affected Version(s): -								
Improper Neutralizat ion of Special Elements used in an OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli-	H-CIS-NEXU- 160323/756				
CVSS Scoring S	icale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	cmdinject- euQVK9u	
Product: ne	xus_3172tq				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/757

0-1

1-2

2-3

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023-		
			20050		
	xus_3172tq-32	lt.			
Affected Ver	sion(s): -		A vulnerability in the		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/758

0-1

1-2

2-3 3-4 4-5 Page 449 of 859 5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_3172tq-xl				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/759

0-1

1-2

2-3

3-4 4-5 Page **450** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	exus_3200				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/760

0-1

1-2

2-3

3-4 4-5 Page **451** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ne	xus_3232c	I		L	L
Affected Vers	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/761
Affected Vers					
Improper Neutralizat ion of Special	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated,	https://sec.clo udapps.cisco.c om/security/c enter/content	H-CIS-NEXU- 160323/762
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 452 of 859	-6 6-7 7-8	<u>8 8-9 9-10</u>

Page 452 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	/CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	
Product: nex	xus_3264c-e				
Affected Vers					
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/763
CVSS Scoring S	cale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne					
Affected Ver	sion(s): -		A vulnerability in the		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/764

0-1

1-2

2-3

3-4 4-5 Page **454** of **859** 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus 3400		20030		
Affected Ver					
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/765

0-1

1-2

2-3

3-4 4-5 Page **455** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne					
Affected Ver	sion(s): -		A vulnerability in the		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/766

0-1

1-2

2-33-44-5Page 456 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the currently logged- in user.		
			CVE ID : CVE-2023- 20050		
Product: nex	xus_34180yc				
Affected Vers	sion(s): -				-
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023 xus_34200yc-s	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/767
Product: nex	xus_34200yc-s	m			

0-1

1-2

2-3

6-7 7-8

5-6

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Version(s): -							
23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/768			
sion(s): - 23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated,	https://sec.clo udapps.cisco.c om/security/c enter/content	H-CIS-NEXU- 160323/769			
	sion(s): - 23-Feb-2023 xus_3432d-s sion(s): -	sion(s): - 23-Feb-2023 7.8 xus_3432d-s sion(s): -	sion(s): -A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system of an affected input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.23-Feb-20237.8A vulnerability in the CLI of Cisco NX-OS Software could allow	sion(s): -A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. An successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system or the underlying operating system ow the the privileges of the currently logged- in user.https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u23-Feb-20237.8K vulnerability in the 			

CVSS Scoring Scale 0-1 1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
used in an OS Command ('OS Command Injection')			execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u			
Product: ne							
Affected Ver	sion(s): -						
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/770		
CVSS Scoring S	Scale 0-1	1-2 2		-6 6-7 7-8	8 8-9 <mark>9-10</mark>		
	Page 459 of 859						

Page **459** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_3500				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/771

0-1

1-2

2-3

3-4 4-5 Page **460** of **859** 6-7

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_3524				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/772

0-1

1-2

2-3

3-4 4-5 Page **461** of **859** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.		
			CVE ID : CVE-2023- 20050		
	exus_3524-x				
Affected Ver	sion(s): -			1	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/773

0-1

1-2

2-3

6-7 7-8

5-6

Product: nex			CVE ID : CVE-2023- 20050 A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated,		
			CLI of Cisco NX-OS Software could allow an authenticated,		
Affected Versi	on(s): -		CLI of Cisco NX-OS Software could allow an authenticated,		
			CLI of Cisco NX-OS Software could allow an authenticated,		
OS Command ('OS Command Injection')	23-Feb-2023	7.8	local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/774
	us_3524-x\/x	1			
Affected Versi	on(s): -				

0-1

1-2

2-3

3-4 4-5 Page **463** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID						
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/775						
	Product: nexus_3548 Affected Version(s): -										
Improper Neutralizat ion of Special Elements used in an OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli-	H-CIS-NEXU- 160323/776						
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 464 of 859	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 ('OS Command Injection')			underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	cmdinject- euQVK9u	
Product: ne	xus_3548-x				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/777

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023-		
Due de et es e			20050		
Affected Ver	xus_3548-xl				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/778

0-1

1-2

2-3 3-4 4-5 Page 466 of 859 5-6

7-8

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_3548-x\/x	:l			
Affected Ver	sion(s): -	-		-	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/779

0-1

1-2

2-3

3-4 4-5 Page **467** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	exus_3600				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/780

0-1

1-2

2-3 3-4 4-5 Page 468 of 859 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Product: ne	xus_36180yc-r	•			I		
Affected Ver	sion(s): -						
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/781		
Product: nexus_3636c-r Affected Version(s): -							
Improper Neutralizat ion of Special	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated,	https://sec.clo udapps.cisco.c om/security/c enter/content	H-CIS-NEXU- 160323/782		

3-4

Page 469 of 859

2-3

4-5

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

0-1

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023-	/CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	
Product: ne	xus 5500		20050		
Affected Vers					
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/783
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10					

Page **470** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_5548p				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/784

0-1

1-2

2-3

3-4 4-5 Page **471** of **859** 6-7

5-6

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_5548up		20030		
Affected Ver	- •				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/785

0-1

1-2

2-3

3-4 4-5 Page **472** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	exus_5596t				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/786

0-1

1-2

2-3 3-4 4-5 Page **473** of **859** 6-7 7-8

5-6

Improper Neutralization of Special Elements23-Feb-2023 20207.8Avulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient vulnerability is due to insufficient vulnerability is the argument of an affected command. A affected command. A successful exploit command (OS Command Injection)7.8Avulnerability is due to insufficient vulnerability is due to insufficient vulnerability bi attacker could attacker to execute argument of an affected command. A successful exploit could allow the attacker to execute argument of an affected command. A successful exploit could allow the attacker to execute argument of an affected command. A successful exploit could allow the attacker to execute argument of an affected command. A successful exploit could allow the attacker to execute argument of an affected command. A successful exploit could allow the attacker to execute argument of an affected command. A successful exploit could allow the arbitrary commands on the underlying operating system with the privileges of in user. CVEID : CVE-2023- cuteH-CIS-NEXU- to insufficient vulnerability by to insufficient vulnerability by operating system with the privileges of in user. CVEID : CVE-2023- cuteH-CIS-NEXU- to insufficient vulnerability by to insufficient vulnerability by operating system with the privileges of in user. cuteH-CIS-NEXU- to insufficient vulnerability by to insufficient vulnerability by operating system with the pri	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an (OS Command Injection')23-Feb-20237.8A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to in sufficient validation of attacker could exposed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. An successful exploit this or same to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient vulnerability by including crafted input as the argument of an affected command. A successful exploit this could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050H-CIS-NEXU- H-CIS-NEXU-<						
Affected Version(s): -A fifected Version(s): -A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could execute arbitrary commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system orsa-nxos-cli- could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of he currently logged- in user.H-CIS-NEXU- 160323/787CVE ID : CVE-2023- 20050CVE ID : CVE-2023- 20050H-CIS-NEXU- 160323/787						
Improper Neutralizat ion of Special Elements used in an Injection')23-Feb-20237.8A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating systemhttps://sec.clo udaps.cisco.c enter/content /CiscoSecurity Advisory/cisc orsa-mos-cli- cm/inject- euQVK9uH-CIS-NEXU- 160323/787Improper Neutralization of successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.https://sec.clo udaps.cisco.c enter/content /CiscoSecurity Advisory/cisc euQVK9uH-CIS-NEXU- 160323/787	Product: ne	xus_5596up				
Improper Neutralizat ion of Special Elements used in an of Software 2014CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.Https://sec.clo udaps.cisco.c om/security/c enter/content /CiscoSecurity devisers/energyH-CIS-NEXU- 160323/787Injection')7.87.87.8H-CIS-NEXU- including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.H-CIS-NEXU- 160323/787	Affected Vers	sion(s): -				
Product: nexus_5600	Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')		7.8	CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023-	udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject-	

0-1

1-2

2-3

3-4 4-5 Page **474** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): -	I			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/788
	xus_56128p				
Affected Ver Improper Neutralizat ion of Special Elements	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity	H-CIS-NEXU- 160323/789

CVSS Scoring Scale 0-1 1-2

5-6

6-7

7-8

8-9

used in an OS Command (OS Command Injection') Product: nexus_5624 Affected Version(s):- Improper Neutralizat ion of Special Elements used in an 2.3-Feb-2023 Command (OS Command 2.3-Feb-2023 Command	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -Improper Neutralizat ion of Special Elements used in an OS Command ['OS Command Injection')A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficienthttps://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9uH-CIS-NEXU- 160323/790	OS Command ('OS Command			commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023-	o-sa-nxos-cli- cmdinject-	
Improper Neutralizat ion of Special Elements used in an OS Command Injection')A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficienthttps://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9uH-CIS-NEXU- 160323/790CVSS Scoring Scale0-11-22-33-44-55-66-77-88-99-10	Product: ne	xus_5624q				
Miniproper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficienthttps://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9uH-CIS-NEXU- 160323/790CVSS Scoring Scale0-11-22-33-44-55-66-77-88-99-10	Affected Ver	sion(s): -				
	Neutralizat ion of Special Elements used in an OS Command ('OS Command	23-Feb-2023	7.8	CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due	udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject-	
Page 476 of 859	CVSS Scoring S	Scale 0-1	1-2 2		<mark>-6 6-7 7-</mark> 8	3 8-9 <mark>9-10</mark>

Page **476** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_5648q				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/791

0-1

1-2

2-3

3-4 4-5 Page **477** of **859** 8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_5672up				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/792

0-1

1-2

2-3

3-4 4-5 Page **478** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.		
			CVE ID : CVE-2023- 20050		
	xus_5672up-1	6g			
Affected Ver	sion(s): -			1	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/793

0-1

1-2

2-3

6-7 7-8

5-6

			Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20050		
Product: ne	xus_5696q				
Affected Vers	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/794
Product: ne	xus_6000				
Affected Vers	sion(s): -				

0-1

1-2

2-3

3-4 4-5 Page **480** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/795			
Product: nexus_6001 Affected Version(s): -								
Improper Neutralizat ion of Special Elements used in an OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli-	H-CIS-NEXU- 160323/796			
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	cmdinject- euQVK9u	
Product: ne	xus_6001p				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/797

0-1

1-2

2-3

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023-		
			20050		
Product: ne					
Affected Verse Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	sion(s): - 23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/798

0-1

1-2

2-33-44-5Page 483 of 859

6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	exus_6004		<u> </u>		
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/799

0-1

1-2

2-3

3-4 4-5 Page **484** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_6004x				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/800

0-1

1-2

2-3

3-4 4-5 Page **485** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Product: ne	xus_7000	I	L				
Affected Ver	sion(s): -						
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/801		
Product: nexus_7004 Affected Version(s): -							
Improper Neutralizat ion of Special	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated,	https://sec.clo udapps.cisco.c om/security/c enter/content	H-CIS-NEXU- 160323/802		

3-4

Page 486 of 859

2-3

4-5

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

0-1

Neutralizat ion ofSoftware could allow an authenticated,udapps.cisco.c om/security/c	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nexus_7009Affected Version(s): -Improper Neutralizat ion of Special Elements used in an OS Command ('OSA vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is duehttps://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9uH-CIS-NEXU- 160323/803	used in an OS Command ('OS Command			execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.	Advisory/cisc o-sa-nxos-cli- cmdinject-	
Affected Version(s): -Improper Neutralizat ion of Special Elements used in an OS Command ('OSA vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is duehttps://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9uH-CIS-NEXU- 160323/803	Product: no	vus 7000		20030		
Improper Neutralizat ion of Special Elements Used in an ('OS23-Feb-20237.8A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, Iocal attacker to execute arbitrary commands on the underlying operating system of an affected device. Thishttps://sec.clo 						
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Improper Neutralizat ion of Special Elements used in an OS Command		7.8	CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This	udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject-	
Page 487 of 859	CVSS Scoring S	Scale 0-1	1-2 2		-6 6-7 7-8	8 8-9 <mark>9-10</mark>

Page **487** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_7010		L	<u> </u>	
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/804

0-1

1-2

2-3 3-4 4-5 Page 488 of 859 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus 7018		20050		
Affected Ver					
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/805

0-1

1-2

2-3

3-4 4-5 Page **489** of **859** 5-6

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
xus_7700				
23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/806
	xus_7700 sion(s): -	xus_7700 sion(s): -	23-Feb-20237.8A vulnerability is due to insufficient validation of a arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the	23-Feb-20237.8A vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could attacker could exploit this vulnerability by including crafted ingust as the argument of an affected command. A successful exploit could allow the attacker to execute argument of an affected command. A successful exploit could allow the attacker to execute argument of an affected commands on the underlying operating systemhttps://sec.clo udaps.cisco.c om/security/c enter/content /CiscoSecurity23-Feb-20237.87.8A vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system

0-1

1-2

2-3 3-4 4-5 Page **490** of **859** 6-7 7-8

5-6

9-10

Improper Neutralizat ion of Special Elements useningXulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to executehttps://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/ciscH-CIS-NEXU- 160323/807	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command Injection')23-Feb-20237.8A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to executehttps://sec.clo udaps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/ciscH-CIS-NEXU- 160323/807						
Affected Version(s): -Affected Version(s): -A fullerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to executehttps://sec.clo udapps.cisco.c om/security/c enter/content /GiscoSecurity Advisory/ciscH-CIS-NEXU- 160323/807						
Improper Neutralizat ion of Special Elements used in an (OS Command (DS Command Injection')7.8A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to executehttps://sec.clo udaps.cisco.c om/security/c enter/content Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9uH-CIS-NEXU- 160323/807	Product: ne	xus_7702				
Improper Neutralizat ion of Special Elements used in an 1njection')23-Feb-20237.8CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of attacker could exploit this vulnerability by including crafted input as the attacker to executeImproper substraint (Cisco Security) Advisory/cisc on-sa-nxos-cli- command affected command. A successful exploit could allow the attacker to executehttps://sec.clo udaps.cisco.c om/security/c enter/content (Cisco Security) Advisory/ciscH-CIS-NEXU- 160323/807	Affected Ver	sion(s): -				
arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')		7.8	CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023-	udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject-	

0-1

1-2

2-3

3-4 4-5 Page **491** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): -	1			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/808
Product: ne					
Affected Vers Improper Neutralizat ion of Special Elements	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity	H-CIS-NEXU- 160323/809

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050	Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	
Product: ne	xus_7718				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/810
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 493 of 859					

Page **493** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	xus_9000		I		
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/811

0-1

1-2

2-3

3-4 4-5 Page **494** of **859** 5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Product: ne	exus_9000v				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	H-CIS-NEXU- 160323/812

0-1

1-2

2-3

3-4 4-5 Page **495** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.		
			CVE ID : CVE-2023- 20050		
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/813

0-1

1-2

2-3

3-4 4-5 Page **496** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Product: ne	xus_92160yc-x	ζ	L		I
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/814

0-1

1-2

2-3

3-4 4-5 Page **497** of **859** 6-7 7-8

5-6

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			parsing ingress LLDP				
			packets. An attacker				
			could exploit this				
			vulnerability by				
			sending a steady				
			stream of crafted				
			LLDP packets to an				
			affected device. A				
			successful exploit				
			could allow the				
			attacker to cause a				
			memory leak, which				
			could result in a				
			denial of service				
			(DoS) condition				
			when the device				
			unexpectedly				
			reloads. Note: This				
			vulnerability cannot				
			be exploited by				
			transit traffic				
			through the device.				
			The crafted LLDP				
			packet must be				
			targeted to a directly				
			connected interface,				
			and the attacker				
			must be in the same				
			broadcast domain as				
			the affected device				
			(Layer 2 adjacent). In				
			addition, the attack surface for this				
			vulnerability can be				
			reduced by disabling LLDP on interfaces				
			where it is not				
			required.				
			CVE ID : CVE-2023-				
			20089				
Product: nexus_92300yc							
Affected Ver	sion(s): -						

0-1

1-2

2-3

3-4 4-5 Page **498** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/815

0-1

1-2

2-3

3-4 4-5 Page **499** of **859** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Product: ne	xus_92304qc				
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/816

0-1

1-2

2-3 3-4 4-5 Page 500 of 859 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Product: ne	xus_92348gc-x	C C			
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/817
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10

Page **501** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to		
			cause a memory leak,		
			which could result in		
			an unexpected		
			reload of the device.		
			This vulnerability is		
			due to incorrect		
			error checking when		
			parsing ingress LLDP		
			packets. An attacker		
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly		
			reloads. Note: This		
			vulnerability cannot		
			be exploited by		
			transit traffic		
			through the device.		
			The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		
			the affected device		
			(Layer 2 adjacent). In		
			addition, the attack		
			surface for this		
			vulnerability can be		
			reduced by disabling		
			LLDP on interfaces		

0-1

1-2

2-33-44-5Page 502 of 859

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			where it is not required. CVE ID : CVE-2023- 20089		
Product: ne	xus_9236c				
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/818

0-1

1-2

2-3

3-4 4-5 Page **503** of **859** 5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Product: ne	NUE 0772		20089		
Affected Ver					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/819

0-1

1-2

2-3

3-4 4-5 Page **504** of **859** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly		
			reloads. Note: This		
			vulnerability cannot		
			be exploited by		
			transit traffic		
			through the device.		
			The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		
			the affected device		
			(Layer 2 adjacent). In		
			addition, the attack		
			surface for this		
			vulnerability can be		
			reduced by disabling		
			LLDP on interfaces		
			where it is not		
			required.		
			CVE ID : CVE-2023-		
			20089		
Product: ne	xus_93108tc-e	X		<u> </u>	
Affected Ver	sion(s): -				
Missing			A vulnerability in the	https://sec.clo	H-CIS-NEXU-
Release of	23-Feb-2023	6.5	Link Layer Discovery	udapps.cisco.c	
Memory			Protocol (LLDP)	om/security/c	160323/820
J	1			, ,,	·
CVSS Scoring S	Scale 0-1	1-2 2		-6 6-7 7-8	8 8-9 9-10
			Page 505 of 859		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
after			feature for Cisco	enter/content	
Effective			Nexus 9000 Series	/CiscoSecurity	
Lifetime			Fabric Switches in	Advisory/cisc	
			Application Centric	o-sa-aci-lldp-	
			Infrastructure (ACI)	dos-	
			Mode could allow an	ySCNZOpX	
			unauthenticated,		
			adjacent attacker to		
			cause a memory leak,		
			which could result in		
			an unexpected		
			reload of the device.		
			This vulnerability is		
			due to incorrect		
			error checking when		
			parsing ingress LLDP		
			packets. An attacker		
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly		
			reloads. Note: This		
			vulnerability cannot		
			be exploited by		
			transit traffic		
			through the device.		
			The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023-		
D	00400	24	20089		
Affected Ver	exus_93108tc-e	x-24			
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/821

0-1

1-2

2-3

3-4 4-5 Page **507** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
	xus_93108tc-fi	x			
Affected Ver	sion(s): -		A 1 1-11		
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/822

0-1

1-2

2-3

3-4 4-5 Page **508** of **859** 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an unexpected		
			reload of the device.		
			This vulnerability is		
			due to incorrect		
			error checking when		
			parsing ingress LLDP		
			packets. An attacker		
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly		
			reloads. Note: This		
			vulnerability cannot		
			be exploited by		
			transit traffic		
			through the device.		
			The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		
			the affected device		
			(Layer 2 adjacent). In		
			addition, the attack		
			surface for this		
			vulnerability can be		
			reduced by disabling		
			LLDP on interfaces		
			where it is not		
			required.		
			-		

0-1

1-2

2-3 3-4 4-5 Page 509 of 859 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			CVE ID : CVE-2023- 20089						
Product: ne	Product: nexus_93108tc-fx-24								
Affected Ver	sion(s): -								
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/823				

0-1

1-2

2-3

3-4 4-5 Page **510** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required.		
			CVE ID : CVE-2023- 20089		
Product: ne	xus_93108tc-f	x3p			
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/824

0-1

1-2

2-33-44-5Page 511 of 859

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Product: ne	xus_93120tx				
Affected Vers	sion(s): -				
Missing Release of Memory after	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity	H-CIS-NEXU- 160323/825
CVSS Scoring S	Scale 0-1	1-2 2	- 3 3-4 4-5 5 Page 512 of 859	-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective			Fabric Switches in	Advisory/cisc	
Lifetime			Application Centric	o-sa-aci-lldp-	
			Infrastructure (ACI)	dos-	
			Mode could allow an	ySCNZOpX	
			unauthenticated,		
			adjacent attacker to		
			cause a memory leak,		
			which could result in		
			an unexpected		
			reload of the device.		
			This vulnerability is		
			due to incorrect		
			error checking when		
			parsing ingress LLDP		
			packets. An attacker		
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly		
			reloads. Note: This		
			vulnerability cannot		
			be exploited by		
			transit traffic		
			through the device.		
			The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		
			the affected device		
			(Layer 2 adjacent). In		

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023-		
			20089		
	exus_93128tx				
Affected Ver			A vulnerability in the		
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/826

0-1

1-2

2-3

3-4 4-5 Page **514** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
	xus_9316d-gx				
Affected Ver	sion(s): -		A mulnorability in the		
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device.	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/827

0-1

1-2

2-3

3-4 4-5 Page **515** of **859** 8-9

9-10

This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted	
error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady	
parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady	
packets. An attacker could exploit this vulnerability by sending a steady	
could exploit this vulnerability by sending a steady	
vulnerability by sending a steady	
sending a steady	
stream of crafted	
Su cam or cratter	
LLDP packets to an	
affected device. A	
successful exploit	
could allow the	
attacker to cause a	
memory leak, which	
could result in a	
denial of service	
(DoS) condition	
when the device	
unexpectedly	
reloads. Note: This	
vulnerability cannot	
be exploited by	
transit traffic	
through the device.	
The crafted LLDP	
packet must be	
targeted to a directly	
connected interface,	
and the attacker	
must be in the same	
broadcast domain as	
the affected device	
(Layer 2 adjacent). In	
addition, the attack	
surface for this	
vulnerability can be	
reduced by disabling	
LLDP on interfaces	
where it is not	
required.	
CVE ID : CVE-2023-	
20089	

0-1

1-2

2-3 3-4 4-5 Page **516** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ne	xus_93180lc-e	x	L	L	
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/828

0-1

1-2

2-3

3-4 4-5 Page **517** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Product: ne	exus_93180yc-e	ex			
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/829

0-1

1-2

2-3 3-4 4-5 Page **518** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Product: ne	xus_93180yc-e	ex-24			
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp-	H-CIS-NEXU- 160323/830
CVSS Scoring S	Scale 0-1	1-2 2		-6 6-7 7-8	8 8-9 9-10

Page **519** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure (ACI)	dos-	
			Mode could allow an	ySCNZOpX	
			unauthenticated,		
			adjacent attacker to		
			cause a memory leak,		
			which could result in		
			an unexpected		
			reload of the device.		
			This vulnerability is		
			due to incorrect		
			error checking when		
			parsing ingress LLDP		
			packets. An attacker		
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly		
			reloads. Note: This		
			vulnerability cannot		
			be exploited by transit traffic		
			through the device. The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		
			the affected device		
			(Layer 2 adjacent). In		
			addition, the attack		
			surface for this		
L			Surface for tills		

0-1

1-2

2-33-44-5Page 520 of 859

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can be reduced by disabling LLDP on interfaces where it is not required.		
			CVE ID : CVE-2023- 20089		
Product: ne	exus_93180yc-f	x	•		•
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/831

0-1

1-2

2-3

3-4 4-5 Page **521** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
	xus_93180yc-f	x-24			
Affected Ver	sion(s): -		A vulnerability in the		
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/832

0-1

1-2

2-3 3-4 4-5 Page **522** of **859**

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			error checking when					
			parsing ingress LLDP					
			packets. An attacker					
			could exploit this					
			vulnerability by					
			sending a steady					
			stream of crafted					
			LLDP packets to an					
			affected device. A					
			successful exploit					
			could allow the					
			attacker to cause a					
			memory leak, which could result in a					
			denial of service					
			(DoS) condition					
			when the device					
			unexpectedly					
			reloads. Note: This					
			vulnerability cannot					
			be exploited by					
			transit traffic					
			through the device.					
			The crafted LLDP					
			packet must be					
			targeted to a directly					
			connected interface,					
			and the attacker					
			must be in the same					
			broadcast domain as					
			the affected device					
			(Layer 2 adjacent). In					
			addition, the attack					
			surface for this					
			vulnerability can be reduced by disabling					
			LLDP on interfaces					
			where it is not					
			required.					
			-					
			CVE ID : CVE-2023-					
D 1	00400		20089					
Product: nexus_93180yc-fx3								
Affected Ver	Affected Version(s): -							
CV/SS Searing (
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 523 of 859								

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/833

0-1

1-2

2-3

3-4 4-5 Page **524** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Improper Authentica tion	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300- FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-elyfex- dos-gfvcByx	H-CIS-NEXU- 160323/834

0-1

1-2

2-33-44-5Page 525 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. CVE ID : CVE-2023- 20012		
Product: ne	exus_93180yc-f	x3s	20012		
Affected Ver					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/835

0-1

1-2

2-3

3-4 4-5 Page **526** of **859** 5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Improper Authentica tion	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300- FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-elyfex- dos-gfvcByx	H-CIS-NEXU- 160323/836

0-1

1-2

2-3

3-4 4-5 Page **527** of **859** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. CVE ID : CVE-2023- 20012		
Product: ne	xus_93216tc-f	x2			
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/837

0-1

1-2

2-3

3-4 4-5 Page **528** of **859** 5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			parsing ingress LLDP					
			packets. An attacker					
			could exploit this					
			vulnerability by					
			sending a steady					
			stream of crafted					
			LLDP packets to an					
			affected device. A					
			successful exploit					
			could allow the					
			attacker to cause a					
			memory leak, which					
			could result in a					
			denial of service					
			(DoS) condition					
			when the device					
			unexpectedly					
			reloads. Note: This					
			vulnerability cannot					
			be exploited by					
			transit traffic					
			through the device.					
			The crafted LLDP					
			packet must be					
			targeted to a directly					
			connected interface,					
			and the attacker					
			must be in the same					
			broadcast domain as					
			the affected device					
			(Layer 2 adjacent). In					
			addition, the attack surface for this					
			vulnerability can be					
			reduced by disabling					
			LLDP on interfaces					
			where it is not					
			required.					
			-					
			CVE ID : CVE-2023-					
			20089					
Product: ne	Product: nexus_93240yc-fx2							
Affected Ver	sion(s): -							

0-1

1-2

2-3

3-4 4-5 Page **529** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/838

0-1

1-2

2-3

3-4 4-5 Page **530** of **859** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Product: ne	xus_9332c				
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/839

0-1

1-2

2-33-44-5Page 531 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Product: ne	xus_9332d-gx2	2b			
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/840
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10
Page 532 of 859					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to		
			cause a memory leak,		
			which could result in		
			an unexpected		
			reload of the device.		
			This vulnerability is		
			due to incorrect		
			error checking when		
			parsing ingress LLDP		
			packets. An attacker		
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition when the device		
			unexpectedly reloads. Note: This		
			vulnerability cannot		
			be exploited by		
			transit traffic		
			through the device.		
			The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		
			the affected device		
			(Layer 2 adjacent). In		
			addition, the attack		
			surface for this		
			vulnerability can be		
			reduced by disabling		
			LLDP on interfaces		

0-1

1-2

2-33-44-5Page 533 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			where it is not required. CVE ID : CVE-2023- 20089		
Product: ne	xus_9332pq				
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/841

0-1

1-2

2-3

3-4 4-5 Page **534** of **859** 5-6

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023-		
Due du et. u e			20089		
Affected Ver	xus_93360yc-f	XZ			
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/842

0-1

1-2

2-33-44-5Page 535 of 859

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly		
			reloads. Note: This		
			vulnerability cannot		
			be exploited by		
			transit traffic		
			through the device.		
			The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		
			the affected device		
			(Layer 2 adjacent). In		
			addition, the attack		
			surface for this		
			vulnerability can be		
			reduced by disabling		
			LLDP on interfaces		
			where it is not		
			required.		
			CVE ID : CVE-2023-		
			20089		
Product: ne	xus_9336c-fx2			<u> </u>	
Affected Vers	sion(s): -				
Missing			A vulnerability in the	https://sec.clo	H-CIS-NEXU-
Release of	23-Feb-2023	6.5	Link Layer Discovery	udapps.cisco.c	
Memory			Protocol (LLDP)	om/security/c	160323/843
J J				, -, -	ıI
CVSS Scoring S	cale 0-1	1-2 2		-6 6-7 7-8	8 8-9 9-10
			Page 536 of 859		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
after			feature for Cisco	enter/content	
Effective			Nexus 9000 Series	/CiscoSecurity	
Lifetime			Fabric Switches in	Advisory/cisc	
			Application Centric	o-sa-aci-lldp-	
			Infrastructure (ACI)	dos-	
			Mode could allow an	ySCNZOpX	
			unauthenticated,		
			adjacent attacker to		
			cause a memory leak,		
			which could result in		
			an unexpected		
			reload of the device.		
			This vulnerability is		
			due to incorrect		
			error checking when		
			parsing ingress LLDP		
			packets. An attacker		
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly		
			reloads. Note: This		
			vulnerability cannot		
			be exploited by		
			transit traffic		
			through the device.		
			The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023-		
Product: ne	exus_9336c-fx2	-0	20089		
Affected Ver		ι 			
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/844

0-1

1-2

2-3

3-4 4-5 Page **538** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
	xus_9336pq_a	ci_spine			
Affected Ver	sion(s): -			I	
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/845

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an unexpected		
			reload of the device.		
			This vulnerability is		
			due to incorrect		
			error checking when		
			parsing ingress LLDP		
			packets. An attacker		
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly		
			reloads. Note: This		
			vulnerability cannot		
			be exploited by		
			transit traffic		
			through the device.		
			The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		
			the affected device		
			(Layer 2 adjacent). In		
			addition, the attack		
			surface for this		
			vulnerability can be		
			reduced by disabling		
			LLDP on interfaces		
			where it is not		
			required.		

0-1

1-2

2-33-44-5Page 540 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20089		
Product: ne	xus_9348d-gx2	2a			
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/846

0-1

1-2

2-33-44-5Page 541 of 859

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required.		
			CVE ID : CVE-2023- 20089		
	xus_9348gc-fx	р			
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/847

0-1

1-2

2-33-44-5Page 542 of 859

6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be treduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023-		
Product: ne	<mark>xus_93600cd-</mark> g	ţx.	20089		
Affected Vers	sion(s): -				
Missing Release of Memory after	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity	H-CIS-NEXU- 160323/848
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 543 of 859	-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective			Fabric Switches in	Advisory/cisc	
Lifetime			Application Centric	o-sa-aci-lldp-	
			Infrastructure (ACI)	dos-	
			Mode could allow an	ySCNZOpX	
			unauthenticated,		
			adjacent attacker to		
			cause a memory leak,		
			which could result in		
			an unexpected		
			reload of the device.		
			This vulnerability is		
			due to incorrect		
			error checking when		
			parsing ingress LLDP		
			packets. An attacker		
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly reloads. Note: This		
			vulnerability cannot		
			be exploited by transit traffic		
			through the device. The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		
			the affected device		
			(Layer 2 adjacent). In		

0-1

1-2

2-3

6-7

7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023-		
Product: ne	9364c		20089		
Affected Ver					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/849

0-1

1-2

2-3

3-4 4-5 Page **545** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
	xus_9364c-gx				
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device.	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/850

0-1

1-2

2-3

3-4 4-5 Page **546** of **859** 6-7 7-8

5-6

8-9 9-10

This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted	
error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady	
parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady	
packets. An attacker could exploit this vulnerability by sending a steady	
could exploit this vulnerability by sending a steady	
vulnerability by sending a steady	
sending a steady	
stream of crafted	
Su cam or cratter	
LLDP packets to an	
affected device. A	
successful exploit	
could allow the	
attacker to cause a	
memory leak, which	
could result in a	
denial of service	
(DoS) condition	
when the device	
unexpectedly	
reloads. Note: This	
vulnerability cannot	
be exploited by	
transit traffic	
through the device.	
The crafted LLDP	
packet must be	
targeted to a directly	
connected interface,	
and the attacker	
must be in the same	
broadcast domain as	
the affected device	
(Layer 2 adjacent). In	
addition, the attack	
surface for this	
vulnerability can be	
reduced by disabling	
LLDP on interfaces	
where it is not	
required.	
CVE ID : CVE-2023-	
20089	

0-1

1-2

2-33-44-5Page 547 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ne	xus_9364d-gx2	2a	L		
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/851

0-1

1-2

2-3

3-4 4-5 Page **548** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023-		
Product: no	xus_9372px		20089		
Affected Ver	-				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/852

0-1

1-2

2-33-44-5Page 549 of 859

6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Product: ne	xus_9372px-e				
Affected Vers	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp-	H-CIS-NEXU- 160323/853
CVSS Scoring S	Scale 0-1	1-2 2	- 3 3-4 4-5 5	-6 6-7 7-6	8 8-9 9-10

Page **550** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	Description & CVE ID Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this	Patch dos- ySCNZOpX	NCIIPC ID

0-1

1-2

2-33-44-5Page 551 of 859

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can be reduced by disabling LLDP on interfaces where it is not required.		
			CVE ID : CVE-2023- 20089		
Product: ne	exus_9372tx				
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/854

0-1

1-2

2-3

3-4 4-5 Page **552** of **859** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
	xus_9372tx-e				
Affected Ver	sion(s): -			1	
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/855

0-1

1-2

2-33-44-5Page 553 of 859

8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	De	scriptio	n & CVE	ID		Patch		NCIIP	CID
					king wh						
			_		gress LL						
			-		n attack	er					
				-	oit this						
				ierabili							
				-	steady						
					crafted						
					ets to ar evice. A	n					
				d allov	exploit						
					cause a						
					ak, whic						
				d resu							
				ial of so							
				S) conc							
			-	n the c							
				xpecte							
				-	ote: This	5					
			vuln	erabili	ity cann	ot					
			be e	xploite	ed by						
			tran	sit traf	ffic						
				-	e device	2.					
					d LLDP						
			_	ket mu							
			-		a direc	-					
					interfac	ce,					
				the att							
					the sam domain						
					d device						
					djacent)						
					he attac						
				ace for		IX .					
					ity can b	be					
					7 disabli						
				-	iterfaces	-					
				ere it is							
			requ	uired.							
			CVE	ID : C	VE-2023	3-					
			200								
Product: ne	xus_9396px										
Affected Ver	sion(s): -										
CVSS Scoring S	Scale 0-1	1-2 2	2-3	3-4	4-5	5-6	6	6-7	7-8	8-9	9-10

Page 554 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/856

0-1

1-2

2-3

3-4 4-5 Page **555** of **859** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Product: ne	xus_9396tx				
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/857

0-1

1-2

2-33-44-5Page 556 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089				
Product: ne	xus_9408			·	·		
Affected Vers	sion(s): -						
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/858		
CVSS Scoring S	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
			adjacent attacker to		
			cause a memory leak,		
			which could result in		
			an unexpected		
			reload of the device.		
			This vulnerability is		
			due to incorrect		
			error checking when		
			parsing ingress LLDP		
			packets. An attacker		
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly reloads. Note: This		
			vulnerability cannot		
			be exploited by transit traffic		
			through the device.		
			The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		
			the affected device		
			(Layer 2 adjacent). In		
			addition, the attack		
			surface for this		
			vulnerability can be		
			reduced by disabling		
			LLDP on interfaces		

0-1

1-2

2-33-44-5Page 558 of 859

6-7

7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			where it is not required. CVE ID : CVE-2023- 20089		
Product: ne	xus_9508	<u> </u>			
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/859

0-1

1-2

2-3

3-4 4-5 Page **559** of **859** 6-7 7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Product: ne	xus_9808				
Affected Ver					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	H-CIS-NEXU- 160323/860

0-1

1-2

2-3

3-4 4-5 Page **560** of **859** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly		
			reloads. Note: This		
			vulnerability cannot		
			be exploited by		
			transit traffic		
			through the device.		
			The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		
			the affected device		
			(Layer 2 adjacent). In		
			addition, the attack		
			surface for this		
			vulnerability can be		
			reduced by disabling		
			LLDP on interfaces		
			where it is not		
			required.		
			CVE ID : CVE-2023-		
			20089		
Product: ucs	s_6200				·
Affected Vers	sion(s): -				
Improper			A vulnerability in the	https://sec.clo	H_CIS_UCS
Neutralizat	23-Feb-2023	6.7	CLI of Cisco	udapps.cisco.c	H-CIS-UCS
ion of			Firepower 4100	om/security/c	160323/861
				,,	1
CVSS Scoring S	cale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	8 8-9 <mark>9-10</mark>
			Page 561 of 859		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special			Series, Cisco	enter/content	
Elements			Firepower 9300	/CiscoSecurity	
used in an			Security Appliances,	Advisory/cisc	
OS			and Cisco UCS 6200,	o-sa-nxfp-	
Command			6300, 6400, and	cmdinj-	
('OS			6500 Series Fabric	XXBZjtR	
Command			Interconnects could		
Injection')			allow an		
			authenticated, local		
			attacker to inject		
			unauthorized		
			commands. This		
			vulnerability is due		
			to insufficient input		
			validation of		
			commands supplied		
			by the user. An		
			attacker could		
			exploit this		
			vulnerability by		
			authenticating to a		
			device and		
			submitting crafted		
			input to the affected		
			command. A		
			successful exploit		
			could allow the		
			attacker to execute		
			unauthorized commands within		
			the CLI. An attacker		
			with Administrator		
			privileges could also		
			execute arbitrary		
			commands on the		
			underlying operating		
			system of Cisco UCS		
			6400 and 6500		
			Series Fabric		
			Interconnects with		
			root-level privileges.		
			CVE ID : CVE-2023-		
			20015		

0-1

1-2

2-33-44-5Page 562 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials.	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-UCS 160323/862

0-1

1-2

2-3

3-4 4-5 Page **563** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20016		
Product: uc	s_6248up				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-UCS 160323/863

0-1

1-2

2-3

3-4 4-5 Page **564** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges.		
			CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-UCS 160323/864

0-1

1-2

2-3

3-4 4-5 Page **565** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Product: uc	:s_6296up				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-UCS 160323/865

0-1

1-2

2-3

3-4 4-5 Page **566** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-UCS 160323/866

0-1

1-2

2-3

3-4 4-5 Page **567** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Product: uc	s 6300		20016		
Affected Ver					
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-UCS 160323/867

0-1

1-2

2-3

3-4 4-5 Page **568** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-UCS 160323/868

0-1

1-2

2-3 3-4 4-5 Page 569 of 859 6-7 7-8

5-6

3-4 4-5 2-3 Page 570 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-UCS 160323/870

0-1

1-2

2-3

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016			
Product: ucs_6332						
Affected Vers	ion(s): -					
Improper Neutralizat ion of Special Elements used in an OS	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp-	H-CIS-UCS 160323/871	
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 ('OS Command Injection')			6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015	cmdinj- XXBZjtR	
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software	https://sec.clo udapps.cisco.c om/security/c enter/content	H-CIS-UCS 160323/872

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			and in the	/CiscoSecurity		
			configuration export	Advisory/cisc		
			feature of Cisco FXOS	o-sa-ucsm-		
			Software could allow	bkpsky-		
			an unauthenticated	H8FCQgsA		
			attacker with access			
			to a backup file to			
			decrypt sensitive			
			information stored in			
			the full state and			
			configuration backup			
			files. This			
			vulnerability is due			
			to a weakness in the			
			encryption method			
			used for the backup			
			function. An attacker			
			could exploit this			
			vulnerability by			
			leveraging a static			
			key used for the			
			backup configuration			
			feature. A successful			
			exploit could allow			
			the attacker to			
			decrypt sensitive			
			information that is			
			stored in full state			
			and configuration			
			backup files, such as local user			
			credentials,			
			authentication			
			server passwords,			
			Simple Network			
			Management			
			Protocol (SNMP)			
			community names,			
			and other			
			credentials.			
			CVE ID : CVE-2023- 20016			
D			20010			
Product: uc	s_6332-16up					

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Ver	Affected Version(s): -								
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-UCS 160323/873				

0-1

1-2

2-33-44-5Page 575 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-UCS 160323/874

0-1

1-2

2-33-44-5Page 576 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Protocol (SNMP) community names, and other credentials.		
			CVE ID : CVE-2023- 20016		
Product: uc	s_64108				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-UCS 160323/875

0-1

1-2

2-3

3-4 4-5 Page **577** of **859** 5-6

6-7 7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-UCS 160323/876

0-1

1-2

2-3

3-4 4-5 Page **578** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Improper Authentica tion	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300- FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-elyfex- dos-gfvcByx	H-CIS-UCS 160323/877

0-1

1-2

2-33-44-5Page 579 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition.		
			CVE ID : CVE-2023- 20012		
Product: uc					
Affected Ver Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-UCS 160323/878
			vulnerability by authenticating to a device and		

0-1

1-2

2-3

3-4 4-5 Page **580** of **859** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-UCS 160323/879

0-1

1-2

2-3

3-4 4-5 Page **581** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Improper Authentica tion	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300- FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-elyfex- dos-gfvcByx	H-CIS-UCS 160323/880

0-1

1-2

2-3

3-4 4-5 Page **582** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. CVE ID : CVE-2023- 20012		
Product: uc	s_6536				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	H-CIS-UCS 160323/881

0-1

1-2

2-3

3-4 4-5 Page **583** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	H-CIS-UCS 160323/882

0-1

1-2

2-3 3-4 4-5 Page **584** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Improper Authentica tion	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300- FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function.	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-elyfex- dos-gfvcByx	H-CIS-UCS 160323/883

0-1

1-2

2-33-44-5Page 585 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. CVE ID : CVE-2023-		
	-		20012		
Vendor: Del Product: a2					
Affected Ver					
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	H-DEL-A200- 160323/884

0-1

1-2

2-3 3-4 4-5 Page 586 of 859 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID Patch		NCIIPC ID
			mechanism causing a denial of service.		
			CVE ID : CVE-2023- 23689		
Product: a2	000				
Affected Ver	sion(s): -				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	H-DEL-A200- 160323/885
Dreduct. f0			23689		
Product: f80 Affected Ver					
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for-	H-DEL-F800- 160323/886

0-1

1-2

2-3

3-4 4-5 Page **587** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	multiple- security	
			CVE ID : CVE-2023- 23689		
Product: f82	-				
Affected Vers Uncontroll ed Resource Consumpti on	sion(s): - 28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	H-DEL-F810- 160323/887
Product: h4	00				
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID Patch		NCIIPC ID
Affected Ver	sion(s): -	L			
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	H-DEL-H400- 160323/888
Product: h5	00				
Affected Ver	sion(s): -				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	H-DEL-H500- 160323/889

0-1

1-2

2-3 3-4 4-5 Page 589 of 859 5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.		
			CVE ID : CVE-2023- 23689		
Product: h5	600				
Affected Ver	sion(s): -				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	H-DEL-H560- 160323/890
Product: h6	00		·		
Affected Ver	sion(s): -				
Uncontroll ed Resource	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810	https://www. dell.com/supp ort/kbdoc/en- us/00020989	H-DEL-H600- 160323/891

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
Consumpti on			integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	
			23689		
Vendor: Dra					
Product: vig	-				
Affected Ver	sion(s): -		A les estilit		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Feb-2023	5.5	A vulnerability classified as problematic has been found in DrayTek Vigor 2960 1.5.1.4. Affected is the function sub_1DF14 of the file /cgi- bin/mainfunction.cgi . The manipulation of the argument option with the input //etc/password leads to path traversal. The attack needs to be done within the local network. The exploit	N/A	H-DRA-VIGO- 160323/892

0-1

1-2

2-33-44-5Page 591 of 859

5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. VDB- 221742 is the identifier assigned to this vulnerability.		
			CVE ID : CVE-2023- 1009		
Vendor: H3	С				
Product: a2	-				
Affected Ver	sion(s): -				
Improper Authentica tion	22-Feb-2023	9.8	An access control issue in H3C A210-G A210-GV100R005 allows attackers to authenticate without a password. CVE ID : CVE-2023- 24093	N/A	H-H3C-A210- 160323/893
Vendor: Ko					
Product: jet Affected Ver					
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294	N/A	H-KOR-JETW- 160323/894
Improper Neutralizat ion of Special Elements used in a	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via	N/A	H-KOR-JETW- 160323/895

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Comman d Injection')			/goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root.		
			CVE ID : CVE-2023- 23295		
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	H-KOR-JETW- 160323/896
Product: jetwave_2111l					
Affected Version(s): -					
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023-	N/A	H-KOR-JETW- 160323/897
			23294		
Improper Neutralizat ion of Special Elements used in a Command ('Comman	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd	N/A	H-KOR-JETW- 160323/898

0-1

1-2

2-33-44-5Page 593 of 859

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			parameter in order to execute commands as root.		
			CVE ID : CVE-2023- 23295		
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t.	N/A	H-KOR-JETW- 160323/899
			CVE ID : CVE-2023- 23296		
Product: jet	wave_2114				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294	N/A	H-KOR-JETW- 160323/900
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root.	N/A	H-KOR-JETW- 160323/901

0-1

1-2

2-3

3-4 4-5 Page **594** of **859** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23295		
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	H-KOR-JETW- 160323/902
Product: jet	wave_2211c				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294	N/A	H-KOR-JETW- 160323/903
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	H-KOR-JETW- 160323/904

0-1

1-2

2-3 3-4 4-5 Page **595** of **859** 5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	H-KOR-JETW- 160323/905
Product: jet	wave_2212g			I	
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294	N/A	H-KOR-JETW- 160323/906
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	H-KOR-JETW- 160323/907
Uncontroll ed Resource	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series	N/A	H-KOR-JETW- 160323/908

0-1

1-2

2-33-44-5Page 596 of 859

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumpti on			1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296		
Product: jet	wave_2212s				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294	N/A	H-KOR-JETW- 160323/909
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	H-KOR-JETW- 160323/910
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via	N/A	H-KOR-JETW- 160323/911

0-1

1-2

2-3

3-4 4-5 Page **597** of **859** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/goform/formDefaul t.		
			CVE ID : CVE-2023- 23296		
Product: jet	wave_2212x				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root.	N/A	H-KOR-JETW- 160323/912
Injection')			CVE ID : CVE-2023- 23294		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	H-KOR-JETW- 160323/913
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t.	N/A	H-KOR-JETW- 160323/914

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Descriptio	n & CVE ID		Patch		NCIIPC ID
			CVE ID : C 23296	VE-2023-				
Product: jet	wave_2411							
Affected Ver	sion(s): -							
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jet 4200 Serie JetWave 30 1.6.0 are v to Comman Injection. A can modify file_name p to execute commands CVE ID : CV 23294	es 1.3.0 and 000 Series ulnerable nd An attacker 7 the parameter 5 as root.		Ą		H-KOR-JETW- 160323/915
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Je 4200 Serie JetWave 30 1.6.0 are v to Comman Injection v /goform/f d. An attac modify the parameter to execute commands CVE ID : C 23295	es 1.3.0 and 000 Series ulnerable nd ia ormSysCm ker an e sysCmd in order s as root.		Ą		H-KOR-JETW- 160323/916
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix Jet 4200 Serie JetWave 32 1.6.0 are ve to Denial o via /goform/fo t. CVE ID : CV 23296	es 1.3.0 and 200 Series ulnerable of Service ormDefaul	N/#	Ą		H-KOR-JETW- 160323/917
Product: jetwave_2411l								
CVSS Scoring S	Scale 0-1	1-2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9 9-10
			5 - 5 -		5.0	07	, 0	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294	N/A	H-KOR-JETW- 160323/918
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	H-KOR-JETW- 160323/919
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	H-KOR-JETW- 160323/920
Product: jet					
Affected Vers	sion(s): -				
Improper Neutralizat	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and	N/A	H-KOR-JETW- 160323/921
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3 3-4 4-5 5</mark> Page 600 of 859	-6 6-7 7-6	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Comman d Injection')			JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	H-KOR-JETW- 160323/922
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	H-KOR-JETW- 160323/923
Product: jet					
Affected Ver	sion(s): -		Koroniy Ist More		
Improper Neutralizat ion of Special Elements	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command	N/A	H-KOR-JETW- 160323/924

 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 in a Command ('Comman d Injection')			Injection. An attacker can modify the file_name parameter to execute commands as root.				
			CVE ID : CVE-2023- 23294				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023-	N/A	H-KOR-JETW- 160323/925		
Uncontroll ed Resource Consumpti on	23-Feb-2023		23295 Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	H-KOR-JETW- 160323/926		
-	Product: jetwave_3220_v3 Affected Version(s): -						
Improper Neutralizat ion of Special Elements used in a Command ('Comman	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter	N/A	H-KOR-JETW- 160323/927		

0-1

1-2

2-3

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			to execute commands as root.		
			CVE ID : CVE-2023- 23294		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	H-KOR-JETW- 160323/928
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	H-KOR-JETW- 160323/929
Product: jet	wave_3420_v3				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root.	N/A	H-KOR-JETW- 160323/930

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23294		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	H-KOR-JETW- 160323/931
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	H-KOR-JETW- 160323/932
Product: jet	wave_4221hp	·е		I	
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294	N/A	H-KOR-JETW- 160323/933

0-1

1-2

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	H-KOR-JETW- 160323/934
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	H-KOR-JETW- 160323/935
Vendor: sic	k				
)-gent00000				
Affected Ver	sion(s): -				
Missing Authentica tion for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GENT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to	https://sick.c om/psirt	H-SIC-FX0 160323/936

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			the listener on TCP port 9000.				
			CVE ID : CVE-2023- 23453				
Product: fx0-gent00010							
Affected Ver	sion(s): -						
Missing Authentica tion for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GENT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000.	https://sick.c om/psirt	H-SIC-FX0 160323/937		
Product: fx(D-gpnt00000		CVE ID : CVE-2023- 23453				
Affected Ver							
			Missing				
Missing Authentica tion for Critical Function	20-Feb-2023	9.8	Authentication for Critical Function in SICK FX0-GPNT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000.	https://sick.c om/psirt	H-SIC-FX0 160323/938		

0-1

1-2

2-3

3-4 4-5 Page **606** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			CVE ID : CVE-2023- 23452						
Product: fx	0-gpnt00010								
Affected Version(s): -									
Missing Authentication for Critical Function in SICK FX0-GPNT v3 									
Vendor: Ter	nda								
Product: ac	500								
Affected Ver	sion(s): -								
Out-of- bounds Write	27-Feb-2023	9.8	Tenda AC500 V2.0.1.9(1307) is vulnerable to Buffer Overflow in function fromRouteStatic via parameters entrys and mitInterface. CVE ID : CVE-2023-	N/A	H-TEN-AC50- 160323/940				
Out-of- bounds Write	27-Feb-2023	9.8	25233 Tenda AC500 V2.0.1.9(1307) is vulnerable to Buffer Overflow in function fromAddressNat via parameters entrys and mitInterface.	N/A	H-TEN-AC50- 160323/941				

0-1

1-2

2-3

5-6 6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25234		
Out-of- bounds Write	27-Feb-2023	7.5	Tenda AC500 V2.0.1.9(1307) is vulnerable to Buffer Overflow in function formOneSsidCfgSet via parameter ssid. CVE ID : CVE-2023- 25235	https://github .com/Funcy33 /Vluninfo_Rep o/tree/main/ CNVDs/113_2	H-TEN-AC50- 160323/942
Product: ax	3				
Affected Ver	sion(s): -				
Out-of- bounds Write	23-Feb-2023	9.8	Tenda AX3 V16.03.12.11 was discovered to contain a stack overflow via the timeType function at /goform/SetSysTime Cfg. CVE ID : CVE-2023- 24212	N/A	H-TEN-AX3- 160323/943
Product: cp	3				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.221 1041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V2022090602 4_2025 and Tenda IT7-PCS Tenda IT7- PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7- LCS<=V2209020914 and Tenda IT7-PRS	N/A	H-TEN-CP3- 160323/944

0-1

1-2

2-3

3-4 4-5 Page **608** of **859** 5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			Tenda IT7- PRS<=V2209020908.			
			CVE ID : CVE-2023- 23080			
Product: cp	7			•		
Affected Ver	sion(s): -				-	
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7 Tenda CP7<=V11.10.00.221 1041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V2022090602 4_2025 and Tenda IT7-PCS Tenda IT7- PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7- LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7- PRS<=V2209020908.	N/A	H-TEN-CP7- 160323/945	
			CVE ID : CVE-2023- 23080			
Product: it7						
Affected Ver	sion(s): -					
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.221 1041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V2022090602 4_2025 and Tenda IT7-PCS Tenda IT7-	N/A	H-TEN-IT7 160323/946	

0-1

1-2

2-3 3-4 4-5 Page 609 of 859 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7- LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7- PRS<=V2209020908.		
			CVE ID : CVE-2023- 23080		
Product: it7	'-pcs				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7 Tenda CP7<=V11.10.00.221 1041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V2022090602 4_2025 and Tenda IT7-PCS Tenda IT7- PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7- LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7- PRS<=V2209020908. CVE ID : CVE-2023- 23080	N/A	H-TEN-IT7 160323/947
Product: it7	<u> </u>				
Affected Ver	sion(s): -		Cortain Tondo		
Improper Neutralizat ion of Special Elements used in a Command	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.221	N/A	H-TEN-IT7 160323/948

 CVSS Scoring Scale
 0-1
 1-2
 2-3
 3-4
 4-5
 5-6

 Page 610 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Comman d Injection')			1041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V2022090602 4_2025 and Tenda IT7-PCS Tenda IT7- PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7- LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7- PRS<=V2209020908. CVE ID : CVE-2023- 23080		
Product: w3	0e		25000		
Affected Vers	sion(s): -				
Out-of- bounds Write	27-Feb-2023	9.8	Tenda Router W30E V1.0.1.25(633) is vulnerable to Buffer Overflow in function fromRouteStatic via parameters entrys and mitInterface. CVE ID : CVE-2023- 25231	N/A	H-TEN-W30E- 160323/949
Vendor: toto	olink			L	I
Product: a7	100ru				
Affected Vers	sion(s): -				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	21-Feb-2023	9.8	TOTOLink A7100RU V7.4cu.2313_B20191 024 was discovered to contain a command injection vulnerability. CVE ID : CVE-2023- 24184	N/A	H-TOT-A710- 160323/950
Improper Neutralizat ion of	16-Feb-2023	9.8	TOTOlink A7100RU(V7.4cu.23 13_B20191024) was	N/A	H-TOT-A710- 160323/951
CVSS Scoring S	cale 0-1	1-2 2	-3 3-4 4-5 5 Page 611 of 859	-6 6-7 7-8	3 8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Special Elements used in a Command ('Comman d Injection')			discovered to contain a command injection vulnerability via the province parameter at setting/delStaticDhc pRules. CVE ID : CVE-2023- 24236			
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	16-Feb-2023	9.8	TOTOlink A7100RU(V7.4cu.23 13_B20191024) was discovered to contain a command injection vulnerability via the city parameter at setting/delStaticDhc pRules. CVE ID : CVE-2023- 24238	N/A	H-TOT-A710- 160323/952	
Product: a7	20r			I	I	
Affected Ver	sion(s): -					
Incorrect Authorizati on	17-Feb-2023	9.8	TOTOLINK A720R V4.1.5cu.532_ B20210610 is vulnerable to Incorrect Access Control. CVE ID : CVE-2023- 23064	N/A	H-TOT-A720- 160323/953	
Vendor: Tp-	link					
Product: ar						
Affected Ver	sion(s): 2					
Improper Resource Shutdown or Release	21-Feb-2023	6.5	A vulnerability was found in TP-Link Archer C50 V2_160801. It has been rated as	N/A	H-TPARCH- 160323/954	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 612 of 859										

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			problematic. Affected by this issue is some unknown functionality of the component Web Management Interface. The manipulation leads to denial of service. The attack can only be initiated within the local network. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221552. CVE ID : CVE-2023- 0936		
Product: tl-	wr940n				
Affected Ver	sion(s): -				
Use of a Broken or Risky Cryptograp hic Algorithm	22-Feb-2023	7.5	TP-Link router TL- WR940N V6 3.19.1 Build 180119 uses a deprecated MD5 algorithm to hash the admin password used for basic authentication.	https://midist 0xf.medium.co m/tl-wr940n- uses-weak- md5-hashing- algorithm- ae7b589860d	H-TPTL-W- 160323/955
			CVE ID : CVE-2023- 23040	2	
Vendor: ui					
Product: un	ifi_dream_mac	hine_pro			
Affected Ver	sion(s): -				
N/A	23-Feb-2023	9.8	Ubiquiti Networks UniFi Dream Machine Pro v7.2.95 allows attackers to bypass domain	N/A	H-UI-UNIF- 160323/956

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 613 of 859										

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restrictions via crafted packets.		
			CVE ID : CVE-2023- 24104		
Vendor: Zyz					
	e3202-m437				
Affected Ver	sion(s): -			1	I
N/A	21-Feb-2023	9.8	A security misconfiguration vulnerability exists in the Zyxel LTE3316-M604 firmware version V2.00(ABMP.6)C0 due to a factory default misconfiguration intended for testing purposes. A remote attacker could leverage this vulnerability to access an affected device using Telnet.	https://www. zyxel.com/glo bal/en/suppo rt/security- advisories/zy xel-security- advisory-for- security- misconfigurati on- vulnerability- of-4g-lte- indoor- routers	H-ZYX-LTE3- 160323/957
			CVE ID : CVE-2023- 22920		
	e3316-m604				
Affected Ver	sion(s): -			T	Γ
N/A	21-Feb-2023	9.8	A security misconfiguration vulnerability exists in the Zyxel LTE3316-M604 firmware version V2.00(ABMP.6)C0 due to a factory default misconfiguration intended for testing purposes. A remote attacker could	https://www. zyxel.com/glo bal/en/suppo rt/security- advisories/zy xel-security- advisory-for- security- misconfigurati on- vulnerability- of-4g-lte-	H-ZYX-LTE3- 160323/958

0-1

1-2

2-3 3-4 4-5 Page 614 of 859 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to access an affected device using Telnet. CVE ID : CVE-2023- 22920	indoor- routers	
			Operating System		
Vendor: abi	15				
Product: tvi	ip_20000-2115	0_firmwa	are		
Affected Ver	sion(s): -				
N/A	27-Feb-2023	7.2	ABUS TVIP 20000- 21150 devices allows remote attackers to execute arbitrary code via shell metacharacters in the /cgi- bin/mft/wireless_mf t ap field. CVE ID : CVE-2023- 26609	N/A	0-ABU-TVIP- 170323/959
Vendor: Ap					
Product: ipa					
Affected Ver	sion(s): * Up to	(excluding	g) 15.7.3		
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges.	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo	0-APP-IPAD- 170323/960

0-1

1-2

2-3

3-4 4-5 Page **615** of **859** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23504	rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to leak sensitive kernel state. CVE ID : CVE-2023- 23500	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	O-APP-IPAD- 170323/961
N/A	27-Feb-2023	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2,	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo	O-APP-IPAD- 170323/962

0-1

1-2

2-3

3-4 4-5 Page **616** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. CVE ID : CVE-2023- 23503	rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	3.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, iOS 16.3 and iPadOS 16.3. The quoted original message may be selected from the wrong email when forwarding an email from an Exchange account. CVE ID : CVE-2023- 23498	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606	O-APP-IPAD- 170323/963
Insertion of Sensitive Informatio n into Log File	27-Feb-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2,	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/	O-APP-IPAD- 170323/964

0-1

1-2

2-3

3-4 4-5 Page **617** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. CVE ID : CVE-2023- 23505	en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213599	
Affected Ver	sion(s): * Up to	(excluding	g) 16.3		
N/A	27-Feb-2023	9.9	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges. CVE ID : CVE-2023- 23531	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606	O-APP-IPAD- 170323/965
N/A	27-Feb-2023	8.8	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2,	https://suppo rt.apple.com/ en- us/HT213605 ,	O-APP-IPAD- 170323/966

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23496	https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599 , https://suppo rt.apple.com/ en- us/HT213600	
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23517	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 ,	O-APP-IPAD- 170323/967

0-1

1-2

2-3

3-4 4-5 Page **619** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23518	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	0-APP-IPAD- 170323/968
N/A	27-Feb-2023	8.6	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code out of	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606	0-APP-IPAD- 170323/969

0-1

1-2

2-33-44-5Page 620 of 859

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			its sandbox or with certain elevated privileges.		
			CVE ID : CVE-2023- 23530		
Out-of- bounds Write	27-Feb-2023	7.5	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Processing an image may lead to a denial- of-service. CVE ID : CVE-2023- 23519	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	O-APP-IPAD- 170323/970
N/A	27-Feb-2023	6.5	The issue was addressed with improved handling of caches. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Visiting a website may lead to an app denial-of- service. CVE ID : CVE-2023- 23512	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	O-APP-IPAD- 170323/971

0-1

1-2

2-33-44-5Page 621 of 859

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of- check Time-of- use (TOCTOU) Race Condition	27-Feb-2023	5.9	A race condition was addressed with additional validation. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. A user may be able to read arbitrary files as root. CVE ID : CVE-2023- 23520	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606	O-APP-IPAD- 170323/972
N/A	27-Feb-2023	5.5	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access user-sensitive data. CVE ID : CVE-2023- 23499	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	0-APP-IPAD- 170323/973
N/A	27-Feb-2023	5.5	An information disclosure issue was	https://suppo rt.apple.com/	O-APP-IPAD- 170323/974

0-1

1-2

2-33-44-5Page 622 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to determine kernel memory layout. CVE ID : CVE-2023- 23502	en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. CVE ID : CVE-2023- 23511	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/	O-APP-IPAD- 170323/975

0-1

1-2

2-33-44-5Page 623 of 859

5-6

6-7

7-8 8-9

3-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en- us/HT213599	
Affected Ver	sion(s): * Up to	(excluding	g) 16.3.1		
Access of Resource Using Incompatib le Type ('Type Confusion')	27-Feb-2023	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, Safari 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited CVE ID : CVE-2023- 23529	https://suppo rt.apple.com/ en- us/HT213638 , https://suppo rt.apple.com/ en- us/HT213635 , https://suppo rt.apple.com/ en- us/HT213633	O-APP-IPAD- 170323/976
Use After Free	27-Feb-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1. An app may be able to execute arbitrary code with kernel privileges CVE ID : CVE-2023- 23514	https://suppo rt.apple.com/ en- us/HT213635 , https://suppo rt.apple.com/ en- us/HT213633	O-APP-IPAD- 170323/977
Uncontroll ed Resource Consumpti on	27-Feb-2023	7.5	A denial-of-service issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.2.1, iOS	https://suppo rt.apple.com/ en- us/HT213634 , https://suppo	O-APP-IPAD- 170323/978

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.3.1 and iPadOS 16.3.1, tvOS 16.3.2, watchOS 9.3.1. Processing a maliciously crafted certificate may lead to a denial-of- service. CVE ID : CVE-2023- 23524	rt.apple.com/ en- us/HT213635 , https://suppo rt.apple.com/ en- us/HT213632 , https://suppo rt.apple.com/ en- us/HT213633	
Affected Ver	sion(s): From (i	ncluding)	16.0 Up to (excluding)	16.3	
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges. CVE ID : CVE-2023- 23504	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	0-APP-IPAD- 170323/979

0-1

1-2

2-33-44-5Page 625 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to leak sensitive kernel state. CVE ID : CVE-2023- 23500	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	O-APP-IPAD- 170323/980
N/A	27-Feb-2023	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. CVE ID : CVE-2023- 23503	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 ,	O-APP-IPAD- 170323/981

0-1

1-2

2-3

3-4 4-5 Page **626** of **859** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	3.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, iOS 16.3 and iPadOS 16.3. The quoted original message may be selected from the wrong email when forwarding an email from an Exchange account. CVE ID : CVE-2023- 23498	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606	O-APP-IPAD- 170323/982
Insertion of Sensitive Informatio n into Log File	27-Feb-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. CVE ID : CVE-2023- 23505	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo	O-APP-IPAD- 170323/983

0-1

1-2

2-3

3-4 4-5 Page **627** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Product: ipl	none os			rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213599				
Affected Version(s): * Up to (excluding) 15.7.3								
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges. CVE ID : CVE-2023- 23504	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	0-APP-IPH0- 170323/984			
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue	https://suppo rt.apple.com/ en- us/HT213598	O-APP-IPHO- 170323/985			
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 628 of 859								

Page 628 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to leak sensitive kernel state. CVE ID : CVE-2023- 23500	, https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. CVE ID : CVE-2023- 23503	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/	0-APP-IPHO- 170323/986

0-1

1-2

2-33-44-5Page 629 of 859

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en- us/HT213599	
N/A	27-Feb-2023	3.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, iOS 16.3 and iPadOS 16.3. The quoted original message may be selected from the wrong email when forwarding an email from an Exchange account. CVE ID : CVE-2023- 23498	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606	O-APP-IPHO- 170323/987
Insertion of Sensitive Informatio n into Log File	27-Feb-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. CVE ID : CVE-2023- 23505	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en-	O-APP-IPHO- 170323/988

0-1

1-2

2-33-44-5Page 630 of 859

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): * Up to	(excluding	g) 16.3	us/HT213604 , https://suppo rt.apple.com/ en- us/HT213599	
			The issue was		
N/A	27-Feb-2023	9.9	addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges. CVE ID : CVE-2023- 23531	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606	O-APP-IPHO- 170323/989
N/A	27-Feb-2023	8.8	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23496	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599 , https://suppo	O-APP-IPHO- 170323/990

0-1

1-2

2-3 3-4 4-5 Page 631 of 859 5-6

6-7

7-8 8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				rt.apple.com/ en- us/HT213600	
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23517	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	0-APP-IPHO- 170323/991
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo	0-APP-IPHO- 170323/992

0-1

1-2

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23518	rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	8.6	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges. CVE ID : CVE-2023- 23530	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606	O-APP-IPHO- 170323/993
Out-of- bounds Write	27-Feb-2023	7.5	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3.	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 ,	O-APP-IPHO- 170323/994

0-1

1-2

2-3

3-4 4-5 Page **633** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Processing an image may lead to a denial- of-service. CVE ID : CVE-2023- 23519	https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	6.5	The issue was addressed with improved handling of caches. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Visiting a website may lead to an app denial-of- service. CVE ID : CVE-2023- 23512	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	0-APP-IPHO- 170323/995
Time-of- check Time-of- use (TOCTOU) Race Condition	27-Feb-2023	5.9	A race condition was addressed with additional validation. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. A user may be able to read arbitrary files as root. CVE ID : CVE-2023- 23520	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606	O-APP-IPHO- 170323/996
N/A	27-Feb-2023	5.5	This issue was addressed by enabling hardened	https://suppo rt.apple.com/ en-	O-APP-IPHO- 170323/997

0-1

1-2

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			runtime. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access user-sensitive data. CVE ID : CVE-2023- 23499	us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601	
N/A	27-Feb-2023	5.5	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to determine kernel memory layout. CVE ID : CVE-2023- 23502	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en-	O-APP-IPHO- 170323/998

0-1

1-2

2-33-44-5Page 635 of 859

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. CVE ID : CVE-2023- 23511	us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599 https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	0-APP-IPHO- 170323/999
Affected Ver	sion(s): * Up to	(excluding	g) 16.3.1	,	
Access of Resource Using Incompatib le Type ('Type Confusion')	27-Feb-2023	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, Safari 16.3. Processing maliciously crafted web content may lead to arbitrary	https://suppo rt.apple.com/ en- us/HT213638 , https://suppo rt.apple.com/ en- us/HT213635 , https://suppo rt.apple.com/	O-APP-IPHO- 170323/1000

0-1

1-2

2-33-44-5Page 636 of 859

5-6

6-7

Free27-Feb-20237.8and iPadOS 16.3.1. An app may be able to execute arbitrary code with kernel privileges.inttps://suppo170323/1001VICONTROLLVERDCVE ID : CVE-2023- 23514inttps://suppointtps://suppoVICONTROLLA denial-of-service issue was addressed with improved input validation. This issue is fixed in macOSinttps://suppointtps://suppoUncontroll ed Resource Consumpti27-Feb-20237.57.5inttps://suppointtps://suppoVICONTROLL27-Feb-20237.57.5inttps://suppointtps://suppointtps://suppoVICONTROLL27-Feb-20237.57.5inttps://suppointtps://suppointtps://suppoVICONTROLL27-Feb-20237.57.5inttps://suppointtps://suppointtps://suppoVICONTROLL27-Feb-20237.57.5inttps://suppointtps://suppointtps://suppoVICONTROLL27-Feb-20237.57.5inttps://suppointtps://suppointtps://suppoVICONTROLL27-Feb-20237.57.5inttps://suppointtps://suppointtps://suppo	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free27-Feb-20237.8A use after free issue was addressed with improved memory management. This issue is fixed in and iPadOS 16.3.1 and iPadOS 16.3.1 and iPadOS 16.3.1 and iPadOS 16.3.1 and iPadOS 16.3.1 and iPadOS 16.3.1 en- us/HT213635 (CVE ID : CVE-2023- 23514https://suppo rt.apple.com/ en- us/HT213633O-APP-IPHO- 170323/1001Uncontroll ed Resource Consumption7.5A denial-of-service issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1, tvOS 16.3.2, watchOS 9.3.1. Processing a maliciously crafted en- us/HT213632https://suppo rt.apple.com/ en- us/HT213634 / https://suppo rt.apple.com/ en- us/HT213634 / https://suppo rt.apple.com/ en- us/HT213634 / https://suppo rt.apple.com/ en- us/HT213634 / https://suppo rt.apple.com/ en- us/HT213634 / https://suppo rt.apple.com/ en- us/HT213634 / https://suppo rt.apple.com/ en- us/HT213634 / https://suppo rt.apple.com/ en- us/HT213635 / https://suppo rt.apple.com/ en- us/HT213634 / https://suppo rt.apple.com/ en- us/HT213634 / https://suppo rt.apple.com/ en- us/HT213634 / https://suppo rt.apple.com/ en-				Apple is aware of a report that this issue may have been		
Use After Free27-Feb-20237.8as addressed with improved memory management. This issue is fixed in and iPadOS 16.3.1. An app may be able to execute arbitrary code with kernel privilegeshttps://suppor rt.apple.com/ en- us/HT213633O-APP-IPHO- 170323/1001Uncontroll ed Resource Consumpti on27-Feb-20237.5A denial-of-service issue was addressed with improved input validation. This issue issue was addressed validation. This issue issue was addressed validation. This issue issue was addressed<						
Uncontroll ed Resource On27-Feb-20237.5A denial-of-service issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, tvOS 16.3.2, watchOS 9.3.1. Processing a maliciously crafted certificate may lead to a denial-of- service.rt.apple.com/ en- us/HT213635 , https://suppo rt.apple.com/ en- us/HT2136320-APP-IPHO- 170323/1002	Use After Free	27-Feb-2023	7.8	was addressed with improved memory management. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1. An app may be able to execute arbitrary code with kernel privileges CVE ID : CVE-2023-	rt.apple.com/ en- us/HT213635 , https://suppo rt.apple.com/ en-	
	Uncontroll ed Resource Consumpti on	27-Feb-2023	7.5	issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, tvOS 16.3.2, watchOS 9.3.1. Processing a maliciously crafted certificate may lead to a denial-of- service. CVE ID : CVE-2023-	rt.apple.com/ en- us/HT213634 , https://suppo rt.apple.com/ en- us/HT213635 , https://suppo rt.apple.com/ en- us/HT213632 , https://suppo rt.apple.com/ en-	
Affected Version(s): From (including) 16.0 Up to (excluding) 16.3	Affected Vers	sion(s): From (i	ncluding)	16.0 Up to (excluding)	16.3	<u> </u>

0-1

1-2

2-3

3-4 4-5 Page **637** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges. CVE ID : CVE-2023- 23504	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	O-APP-IPHO- 170323/1003
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to leak sensitive kernel state.	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 ,	O-APP-IPHO- 170323/1004

0-1

1-2

2-3

3-4 4-5 Page **638** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23500	https://suppo rt.apple.com/ en- us/HT213601	
				https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. CVE ID : CVE-2023- 23503	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/	O-APP-IPHO- 170323/1005
N/A	27-Feb-2023	3.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2,	en- us/HT213599 https://suppo rt.apple.com/ en- us/HT213598 , https://suppo	O-APP-IPHO- 170323/1006
			iOS 15.7.3 and iPadOS 15.7.3, iOS 16.3 and iPadOS 16.3. The quoted	rt.apple.com/ en- us/HT213605 ,	

0-1

1-2

2-33-44-5Page 639 of 859

5-6

Insertion of Sensitive Information n into Log FileZ7-Feb-2023 3.3a.8A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in maCOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, maCOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, maCOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, maCOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, maCOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. CVE ID : CVE-2023- 23505https://suppo rt.apple.com/ en- us/HT213606 https://suppo rt.apple.com/ en- us/HT2136060-APP-IPHO- 170323/1007Product: macosTorke 2023 and iPadOS 16.3 and iPadOS 17.323/10070-APP-IPHO- 170323/1007Product: macosTorke 2023- 23505Improve and iPadOS 17.323/10070-APP-MACO- 170323/1008Improve Typer Imput Validation17-Feb-2023 7.87.8Photoshop version 23.51 (and earlier), 24.1 (and earlier) are curity/produchttps://helpx. adobe.com/se curity/produc	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Informatio n into Log27-Feb-20233.3A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Monterey 12.6.3, iOS 15.7.3 matOS Sensitive Informatio n into Loghttps://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213606 into LogO-APP-IPHO- informatio rapile.com/ en- us/HT213606 information about a user's contacts. CVE ID : CVE-2023- 23505O-APP-IPHO- information about a us/HT213604 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apile.com/ en- us/HT213604 , https://suppo rt.apile.com/ en- us/HT213604 , https://suppo rt.apile.com/ en- us/HT213604 , https://suppo rt.apile.com/ en- us/HT213604 , https://suppo rt.apile.com/ en- us/HT213599O-APP-MACO- 170323/1008				may be selected from the wrong email when forwarding an email from an Exchange account.	rt.apple.com/ en-	
Insertion of Sensitive Information ninto Log27-Feb-20233.3A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 15.7.3, 						
Affected Version(s): -Improper Input17-Feb-20237.8Photoshop version 23.5.3 (and earlier),https://helpx. adobe.com/se0-APP-MACO- 170323/1008	of Sensitive Informatio n into Log File		3.3	addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. CVE ID : CVE-2023-	rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en-	
Improper Input17-Feb-20237.8Photoshop version 23.5.3 (and earlier),https://helpx. adobe.com/se0-APP-MACO- 170323/1008						
	Improper Input		7.8	23.5.3 (and earlier),	adobe.com/se	

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
			affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21574	ts/photoshop /apsb23- 11.html	
Out-of- bounds Write	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21575	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	O-APP-MACO- 170323/1009
Out-of- bounds Write	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	O-APP-MACO- 170323/1010

0-1

1-2

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21576		
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by a Stack- based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22226	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	O-APP-MACO- 170323/1011
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	O-APP-MACO- 170323/1012

0-1

1-2

2-3

3-4 4-5 Page **642** of **859** 6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2023- 22227		
Improper Input Validation	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22228	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	O-APP-MACO- 170323/1013
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	O-APP-MACO- 170323/1014

0-1

1-2

2-3

3-4 4-5 Page **643** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22229		
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22230	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	O-APP-MACO- 170323/1015
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Heap- based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22236	https://helpx. adobe.com/se curity/produc ts/animate/ap sb23-15.html	O-APP-MACO- 170323/1016

0-1

1-2

2-3 3-4 4-5 Page 644 of 859 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22237	https://helpx. adobe.com/se curity/produc ts/after_effect s/apsb23- 02.html	O-APP-MACO- 170323/1017
Out-of- bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22238	https://helpx. adobe.com/se curity/produc ts/after_effect s/apsb23- 02.html	O-APP-MACO- 170323/1018
Improper Input Validation	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an Improper Input Validation vulnerability that	https://helpx. adobe.com/se curity/produc ts/after_effect s/apsb23- 02.html	O-APP-MACO- 170323/1019

0-1

1-2

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-		
Out-of- bounds Write	17-Feb-2023	7.8	22239 Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Stack- based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22243	https://helpx. adobe.com/se curity/produc ts/animate/ap sb23-15.html	O-APP-MACO- 170323/1020
Use After Free	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the	https://helpx. adobe.com/se curity/produc ts/animate/ap sb23-15.html	O-APP-MACO- 170323/1021

0-1

1-2

3-4 4-5 2-3 Page 646 of 859

5-6 6-7 7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2023- 22246		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Crafter Studio on Linux, MacOS, Windows, x86, ARM, 64 bit allows SQL Injection.This issue affects CrafterCMS v4.0 from 4.0.0 through 4.0.1, and v3.1 from 3.1.0 through 3.1.26. CVE ID : CVE-2023- 26020	https://docs.c raftercms.org /en/4.0/secur ity/advisory.h tml#cv- 2023021701	O-APP-MACO- 170323/1022
Out-of- bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of- bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	O-APP-MACO- 170323/1023

0-1

1-2

2-3

3-4 4-5 Page **647** of **859** 7-8

6-7

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2023- 21577		
Out-of- bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of- bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	O-APP-MACO- 170323/1024
			CVE ID : CVE-2023- 21578		
Out-of- bounds Read	17-Feb-2023	5.5	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	O-APP-MACO- 170323/1025

0-1

1-2

2-3

3-4 4-5 Page **648** of **859** 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2023- 21583		
NULL Pointer Dereferenc e	17-Feb-2023	5.5	Adobe InDesign versions ID18.1 (and earlier) and ID17.4 (and earlier) are affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of- service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-	https://helpx. adobe.com/se curity/produc ts/indesign/a psb23- 12.html	O-APP-MACO- 170323/1026
Out-of- bounds Read	17-Feb-2023	5.5	21593 Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	O-APP-MACO- 170323/1027

0-1

1-2

2-3

3-4 4-5 Page **649** of **859** 6-7 7-8

5-6

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22231		
Out-of- bounds Read	17-Feb-2023	5.5	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22233	https://helpx. adobe.com/se curity/produc ts/after_effect s/apsb23- 02.html	O-APP-MACO- 170323/1028
Affected Ver	sion(s): * Up to	(excluding	g) 11.7.3		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	27-Feb-2023	9.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. Mounting a maliciously crafted Samba network share may lead to arbitrary code execution.	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604	O-APP-MACO- 170323/1029

0-1

1-2

2-33-44-5Page 650 of 859

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23513		
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23517	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	O-APP-MACO- 170323/1030
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/	O-APP-MACO- 170323/1031

0-1

1-2

2-33-44-5Page 651 of 859

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23518	en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
Affected Ver	sion(s): * Up to	(excluding	g) 13.2		
N/A	27-Feb-2023	9.9	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges. CVE ID : CVE-2023- 23531	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606	O-APP-MACO- 170323/1032
N/A	27-Feb-2023	8.8	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. Processing maliciously crafted	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 ,	O-APP-MACO- 170323/1033

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23496	https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599 , https://suppo rt.apple.com/ en- us/HT213600	
N/A	27-Feb-2023	8.6	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges. CVE ID : CVE-2023- 23530	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606	O-APP-MACO- 170323/1034
Out-of- bounds Write	27-Feb-2023	7.5	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Processing an image may lead to a denial- of-service.	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601	O-APP-MACO- 170323/1035

0-1

1-2

2-33-44-5Page 653 of 859

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23519	, https://suppo rt.apple.com/ en- us/HT213599	
Time-of- check Time-of- use (TOCTOU) Race Condition	27-Feb-2023	5.9	A race condition was addressed with additional validation. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. A user may be able to read arbitrary files as root. CVE ID : CVE-2023- 23520	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606	O-APP-MACO- 170323/1036
Exposure of Resource to Wrong Sphere	27-Feb-2023	5.5	The issue was addressed with improved memory handling This issue is fixed in macOS Ventura 13.2. An app may be able to disclose kernel memory CVE ID : CVE-2023- 23501	https://suppo rt.apple.com/ en- us/HT213605	O-APP-MACO- 170323/1037
N/A	27-Feb-2023	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences.	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606	O-APP-MACO- 170323/1038

0-1

1-2

2-33-44-5Page 654 of 859

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23503	, https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	5.5	A permissions issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.2. An app may be able to access user- sensitive data. CVE ID : CVE-2023- 23506	https://suppo rt.apple.com/ en- us/HT213605	O-APP-MACO- 170323/1039
N/A	27-Feb-2023	5.5	A permissions issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.2. An app may be able to access a user's Safari history. CVE ID : CVE-2023- 23510	https://suppo rt.apple.com/ en- us/HT213605	O-APP-MACO- 170323/1040
N/A	27-Feb-2023	5.5	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Ventura 13.2.1. An app may be able to observe unprotected user data CVE ID : CVE-2023- 23522	https://suppo rt.apple.com/ en- us/HT213633	O-APP-MACO- 170323/1041

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Ver	sion(s): * Up to	(excluding	g) 13.2.1				
Access of Resource Using Incompatib le Type ('Type Confusion')	27-Feb-2023	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, Safari 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited CVE ID : CVE-2023- 23529	https://suppo rt.apple.com/ en- us/HT213638 , https://suppo rt.apple.com/ en- us/HT213635 , https://suppo rt.apple.com/ en- us/HT213633	O-APP-MACO- 170323/1042		
Uncontroll ed Resource Consumpti on	27-Feb-2023	7.5	A denial-of-service issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, tvOS 16.3.2, watchOS 9.3.1. Processing a maliciously crafted certificate may lead to a denial-of- service. CVE ID : CVE-2023- 23524	https://suppo rt.apple.com/ en- us/HT213634 , https://suppo rt.apple.com/ en- us/HT213635 , https://suppo rt.apple.com/ en- us/HT213632 , https://suppo rt.apple.com/ en- us/HT213633	O-APP-MACO- 170323/1043		
Affected Ver	Affected Version(s): From (including) 11.0 Up to (excluding) 11.7.3						
N/A	27-Feb-2023	7.8	A logic issue was addressed with	https://suppo rt.apple.com/	0-APP-MACO- 170323/1044		

0-1

1-2

2-33-44-5Page 656 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved state management. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. An app may be able to gain root privileges. CVE ID : CVE-2023- 23497	en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604	
N/A	27-Feb-2023	5.5	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access user-sensitive data. CVE ID : CVE-2023- 23499	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	O-APP-MACO- 170323/1045
N/A	27-Feb-2023	5.5	The issue was addressed with	https://suppo rt.apple.com/	O-APP-MACO- 170323/1046

0-1

1-2

2-33-44-5Page 657 of 859

5-6

6-7

Insertion of Sensitive Informatio ni tub Log File27-Feb-2023 23-505a.aA privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sig Suren- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604O-APP-MACO- 170323/1047Insertion of Sensitive Informatio ni into Log File27-Feb-2023 2.3-Feb-20233.3A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, IOS 15.7.3, watchOS 9.3, IOS 16.3 and iPadOS 15.7.3, watchOS 9.3, IOS 16.3, and IPadOS 15.7.3, watc	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Informatio n into Log File27-Feb-20233.3A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts.o-APP-MACO- 170323/1047O-APP-MACO- 170323/10470-APP-MACO- 170323/1047				handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. An app may be able to bypass Privacy preferences. CVE ID : CVE-2023-	us/HT213605 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en-	
	of Sensitive Informatio n into Log File			addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. CVE ID : CVE-2023- 23505	rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213604	

0-1

1-2

2-33-44-5Page 658 of 859

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	27-Feb-2023	9.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. Mounting a maliciously crafted Samba network share may lead to arbitrary code execution. CVE ID : CVE-2023- 23513	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604	O-APP-MACO- 170323/1048
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23517	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en-	O-APP-MACO- 170323/1049

0-1

1-2

2-33-44-5Page 659 of 859

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID							
				en- us/HT213599								
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23518	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	O-APP-MACO- 170323/1050							
Affected Ver	sion(s): From (i	ncluding)	12.0.0 Up to (excluding	g) 12.6.3								
N/A	27-Feb-2023	7.8	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. An app may be able to gain root privileges.	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo	O-APP-MACO- 170323/1051							
CV/SS Scoring S		1_2			8 8-9 0.10							
		1-2 2	Page 660 of 859		CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10							

Page 660 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23497	rt.apple.com/ en- us/HT213604	
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges. CVE ID : CVE-2023- 23504	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601	O-APP-MACO- 170323/1052
N/A	27-Feb-2023	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3. An app may be able to execute arbitrary code with kernel privileges.	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213604	O-APP-MACO- 170323/1053

0-1

1-2

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23507		
N/A	27-Feb-2023	5.5	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access user-sensitive data. CVE ID : CVE-2023- 23499	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	O-APP-MACO- 170323/1054
N/A	27-Feb-2023	5.5	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/	O-APP-MACO- 170323/1055

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to determine kernel memory layout. CVE ID : CVE-2023- 23502	en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. An app may be able to bypass Privacy preferences. CVE ID : CVE-2023- 23508	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604	0-APP-MACO- 170323/1056
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. CVE ID : CVE-2023- 23511	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/	O-APP-MACO- 170323/1057

0-1

1-2

2-33-44-5Page 663 of 859

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
Improper Authentica tion	27-Feb-2023	3.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3. An encrypted volume may be unmounted and remounted by a different user without prompting for the password. CVE ID : CVE-2023- 23493	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213604	O-APP-MACO- 170323/1058
Insertion of Sensitive Informatio n into Log File	27-Feb-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. CVE ID : CVE-2023- 23505	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 ,	O-APP-MACO- 170323/1059

0-1

1-2

2-3 3-4 4-5 Page 664 of 859 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s). From (i	ncluding)	13.0 Up to (excluding)	https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213599	
Affected Version(s): From (including) 13.0 Up to (excluding) 13.2 A buffer overflow					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	27-Feb-2023	9.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. Mounting a maliciously crafted Samba network share may lead to arbitrary code execution. CVE ID : CVE-2023- 23513	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604	O-APP-MACO- 170323/1060
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Wonterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution.	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/	O-APP-MACO- 170323/1061

0-1

1-2

2-3

3-4 4-5 Page **665** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23517	en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23518	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	0-APP-MACO- 170323/1062
N/A	27-Feb-2023	7.8	A logic issue was addressed with	https://suppo rt.apple.com/	0-APP-MACO- 170323/1063

0-1

1-2

3-4 4-5 2-3 Page 666 of 859

5-6

6-7

8-9

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved state management. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. An app may be able to gain root privileges. CVE ID : CVE-2023- 23497	en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604	
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges. CVE ID : CVE-2023- 23504	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	0-APP-MACO- 170323/1064
N/A	27-Feb-2023	7.8	The issue was addressed with	https://suppo rt.apple.com/	O-APP-MACO- 170323/1065

0-1

1-2

2-3 3-4 4-5 Page 667 of 859 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved bounds checks. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3. An app may be able to execute arbitrary code with kernel privileges. CVE ID : CVE-2023- 23507	en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213604	
N/A	27-Feb-2023	6.5	The issue was addressed with improved handling of caches. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Visiting a website may lead to an app denial-of- service. CVE ID : CVE-2023- 23512	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	O-APP-MACO- 170323/1066
N/A	27-Feb-2023	5.5	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en-	O-APP-MACO- 170323/1067

0-1

1-2

2-3 3-4 4-5 Page **668** of **859** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access user-sensitive data. CVE ID : CVE-2023- 23499	us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to leak sensitive kernel state. CVE ID : CVE-2023- 23500	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	O-APP-MACO- 170323/1068
N/A	27-Feb-2023	5.5	An information disclosure issue was addressed by	https://suppo rt.apple.com/ en-	O-APP-MACO- 170323/1069

0-1

1-2

2-3 3-4 4-5 Page 669 of 859 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removing the vulnerable code. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to determine kernel memory layout. CVE ID : CVE-2023- 23502	us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. An app may be able to bypass Privacy preferences. CVE ID : CVE-2023- 23508	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604	O-APP-MACO- 170323/1070
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en-	O-APP-MACO- 170323/1071

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. CVE ID : CVE-2023- 23511	us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
Improper Authentica tion	27-Feb-2023	3.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3. An encrypted volume may be unmounted and remounted by a different user without prompting for the password. CVE ID : CVE-2023- 23493	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213604	O-APP-MACO- 170323/1072
N/A	27-Feb-2023	3.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, iOS 16.3 and iPadOS 16.3. The quoted original message	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo	O-APP-MACO- 170323/1073

0-1

1-2

2-33-44-5Page 671 of 859

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be selected from the wrong email when forwarding an email from an Exchange account. CVE ID : CVE-2023- 23498	rt.apple.com/ en- us/HT213606	
Insertion of Sensitive Informatio n into Log File	27-Feb-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. CVE ID : CVE-2023- 23505	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213604	O-APP-MACO- 170323/1074
Affected Vers	sion(s): From (i	ncluding)	13.0 Up to (excluding)	-	1
Use After Free	27-Feb-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura	https://suppo rt.apple.com/ en- us/HT213635 , https://suppo	O-APP-MACO- 170323/1075
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	<u>8-9 9-10</u>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13.2.1, iOS 16.3.1 and iPadOS 16.3.1. An app may be able to execute arbitrary code with kernel privileges CVE ID : CVE-2023-	rt.apple.com/ en- us/HT213633	
			23514		
Product: tvo		<u>());</u>			
Affected Ver	sion(s): * Up to	(excluding	g) 16.3		
N/A	27-Feb-2023	8.8	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23496	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599 , https://suppo rt.apple.com/ en- us/HT213600	0-APP-TVOS- 170323/1076
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en-	O-APP-TVOS- 170323/1077

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23517	us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23518	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213604	O-APP-TVOS- 170323/1078

0-1

1-2

2-3

3-4 4-5 Page **674** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599 https://suppo rt.apple.com/	
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges. CVE ID : CVE-2023- 23504	en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601	O-APP-TVOS- 170323/1079
Out-of- bounds Write	27-Feb-2023	7.5	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en-	0-APP-TVOS- 170323/1080

0-1

1-2

2-3

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and iPadOS 16.3, watchOS 9.3. Processing an image may lead to a denial- of-service. CVE ID : CVE-2023- 23519	us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	6.5	The issue was addressed with improved handling of caches. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Visiting a website may lead to an app denial-of- service. CVE ID : CVE-2023- 23512	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	O-APP-TVOS- 170323/1081
N/A	27-Feb-2023	5.5	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en-	0-APP-TVOS- 170323/1082

0-1

1-2

2-3

3-4 4-5 Page **676** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access user-sensitive data. CVE ID : CVE-2023- 23499	us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to leak sensitive kernel state. CVE ID : CVE-2023- 23500	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601	O-APP-TVOS- 170323/1083
N/A	27-Feb-2023	5.5	An information disclosure issue was addressed by	https://suppo rt.apple.com/ en-	O-APP-TVOS- 170323/1084

0-1

1-2

2-33-44-5Page 677 of 859

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removing the vulnerable code. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to determine kernel memory layout. CVE ID : CVE-2023- 23502	us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213609	
N/A	27-Feb-2023	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. CVE ID : CVE-2023- 23503	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/	O-APP-TVOS- 170323/1085

0-1

1-2

2-33-44-5Page 678 of 859

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en- us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. CVE ID : CVE-2023- 23511	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	0-APP-TVOS- 170323/1086
Affected Ver	sion(s): * Up to	(excluding	g) 16.3.2	1	
Uncontroll ed Resource Consumpti on	27-Feb-2023	7.5	A denial-of-service issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, tvOS 16.3.2, watchOS 9.3.1. Processing a maliciously crafted certificate may lead to a denial-of- service.	https://suppo rt.apple.com/ en- us/HT213634 , https://suppo rt.apple.com/ en- us/HT213635 , https://suppo rt.apple.com/ en- us/HT213632 , https://suppo	0-APP-TVOS- 170323/1087

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2023- 23524	rt.apple.com/ en- us/HT213633						
Product: wa	atchos			·						
Affected Ver	Affected Version(s): * Up to (excluding) 9.3									
N/A	27-Feb-2023	8.8	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23496	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599 , https://suppo rt.apple.com/ en- us/HT213600	0-APP-WATC- 170323/1088					
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603	O-APP-WATC- 170323/1089					

0-1

1-2

2-3 3-4 4-5 Page **680** of **859** 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. CVE ID : CVE-2023- 23517	, https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2023- 23518	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601	0-APP-WATC- 170323/1090

0-1

1-2

2-33-44-5Page 681 of 859

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en- us/HT213599	
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges. CVE ID : CVE-2023- 23504	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213601 ,	0-APP-WATC- 170323/1091
Out-of- bounds Write	27-Feb-2023	7.5	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Processing an image	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/	0-APP-WATC- 170323/1092

0-1

1-2

2-3

5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may lead to a denial- of-service. CVE ID : CVE-2023- 23519	en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	6.5	The issue was addressed with improved handling of caches. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Visiting a website may lead to an app denial-of- service. CVE ID : CVE-2023- 23512	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	0-APP-WATC- 170323/1093
N/A	27-Feb-2023	5.5	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access user-sensitive data. CVE ID : CVE-2023- 23499	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/	O-APP-WATC- 170323/1094

0-1

1-2

2-33-44-5Page 683 of 859

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to leak sensitive kernel state. CVE ID : CVE-2023- 23500	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	O-APP-WATC- 170323/1095
N/A	27-Feb-2023	5.5	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.2,	https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/	O-APP-WATC- 170323/1096

0-1

1-2

2-3 3-4 4-5 Page **684** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to determine kernel memory layout. CVE ID : CVE-2023- 23502	en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
N/A	27-Feb-2023	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. CVE ID : CVE-2023- 23503	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	O-APP-WATC- 170323/1097
N/A	27-Feb-2023	5.5	The issue was addressed with	https://suppo rt.apple.com/	0-APP-WATC- 170323/1098

0-1

1-2

2-3 3-4 4-5 Page 685 of 859 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. CVE ID : CVE-2023- 23511	en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213601 , https://suppo rt.apple.com/ en- us/HT213599	
Insertion of Sensitive Informatio n into Log File	27-Feb-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. CVE ID : CVE-2023- 23505	https://suppo rt.apple.com/ en- us/HT213598 , https://suppo rt.apple.com/ en- us/HT213605 , https://suppo rt.apple.com/ en- us/HT213606 , https://suppo rt.apple.com/ en- us/HT213603 , https://suppo rt.apple.com/ en-	O-APP-WATC- 170323/1099

0-1

1-2

2-3

3-4 4-5 Page **686** of **859** 5-6

6-7

9-10

	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	ion(s): * Up to	(oxcludin)	n) 0 2 1	en- us/HT213604 , https://suppo rt.apple.com/ en- us/HT213599	
Allected versi		(excluding	gj 9.3.1	1	
Consumpti on	27-Feb-2023	7.5	A denial-of-service issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, tvOS 16.3.2, watchOS 9.3.1. Processing a maliciously crafted certificate may lead to a denial-of- service. CVE ID : CVE-2023- 23524	https://suppo rt.apple.com/ en- us/HT213634 , https://suppo rt.apple.com/ en- us/HT213635 , https://suppo rt.apple.com/ en- us/HT213632 , https://suppo rt.apple.com/ en- us/HT213633	0-APP-WATC- 170323/1100
Vendor: Asus	S				
Product: asm	1b8-ikvm_firm	iware			
Affected Versi	ion(s): * Up to	(including	g) 1.14.51		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	26-Feb-2023	9.8	ASUS ASMB8 iKVM firmware through 1.14.51 allows remote attackers to execute arbitrary code by using SNMP to create extensions, as demonstrated by snmpset for NET- SNMP-EXTEND-MIB with /bin/sh for command execution.	N/A	0-ASU-ASMB- 170323/1101
			<mark>-3</mark> 3-4 4-5 5	-6 6-7 7-8	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 26602		
Vendor: Axi	S				
Product: 20	7w_firmware				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	6.1	** UNSUPPORTED WHEN ASSIGNED ** A Vulnerability was discovered in Axis 207W network camera. There is a reflected XSS vulnerability in the web administration portal, which allows an attacker to execute arbitrary JavaScript via URL. CVE ID : CVE-2023- 22984	N/A	0-AXI-207W- 170323/1102
Vendor: Cis					
Product: fxo					
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	0-CIS-FXOS- 170323/1103

0-1

1-2

2-3 3-4 4-5 Page **688** of **859** 6-7

5-6

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges.		
Affected Ver	cion(c), * Un to	(oveludin	20015		
Allected ver	sion(s): * Up to	(excluding	A vulnerability in the		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	O-CIS-FXOS- 170323/1104

0-1

1-2

2-3

3-4 4-5 Page **689** of **859** 5-6

7-8

Weakness	Publish Date	CVSSv3	D	escriptio	n & CVE II	D		Patch		1	ICIIP	CID	
			file vul to a end use fun cou vul lev key bad fea exp the ded inf sto and bad loc cre aut ser Sim Ma Pro cor and cor	es. This inerabilities a weaking cryption ed for the action. A ald exploit eraging y used for chup con- ture. A se oloit courte attacket crypt ser ormation red in fur d config chup file al user edentials chentica wer passe inple Net inageme otocol (Si inmunity d other edentials	ty by a static or the figuratio successfu- ld allow er to nsitive n that is all state uration s, such a s, tion swords, work nt SMMP) y names,	e e er on al							
			20	016									
Product: ne	xus_93180yc-f	x3s_firm	war	e									
Affected Ver	sion(s): -												
Improper Authentica tion	23-Feb-2023	4.6	CLI aut Cis FX Ext wh Fal	l console chentica co Nexu 3 Series cender (en used oric Inte	tion of s 9300- Fabric FEX)	t	uda om, ente /Cis Adv o-sa	os://se pps.cis /securi er/cont scoSecu visory/o a-elyfex -gfvcBy	ty/c tent trity cisc	0-CI 1703		XU- 1105	
CVSS Scoring S	Scale 0-1	1-2	2-3	3-4	4-5	5-	6	6-7	7-8	3	8-9	9-10	

Page 690 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. CVE ID : CVE-2023- 20012		
Product: ne	xus_93180yc-f	x3_firmw	are		
Affected Ver	sion(s): -				
Improper Authentica tion	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300- FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-elyfex- dos-gfvcByx	O-CIS-NEXU- 170323/1106
		1 2			
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5 Page 691 of 859	<mark>-6 6-7 7-</mark> 8	8-9 9-10

Page 691 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. CVE ID : CVE-2023- 20012		
Product: nx	-05				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	O-CIS-NX-O- 170323/1107

0-1

1-2

2-3

3-4 4-5 Page **692** of **859** 5-6 6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Affected Ver	sion(s): * Up to	(excluding	g) 10.2\\(4\\)		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	O-CIS-NX-O- 170323/1108

0-1

1-2

2-33-44-5Page 693 of 859

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023- 20050		
Affected Ver	sion(s): * Up to	(excluding			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject- euQVK9u	0-CIS-NX-0- 170323/1109

0-1

1-2

2-3 3-4 4-5 Page 694 of 859 6-7 7-8

5-6

9-10

Affected Version(s): * Up to (excluding) 9.3\(10\)Affected Version(s): * Up to (excluding) 9.3\(10\)Affected Version(s): * Up to (excluding) 9.3\(10\)Affected Version(s): * Up to (excluding) 9.3\(10\)A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI of arguments that are passed to specific CLI odvisory/cisc o-CIS-NX-O- 170323/1110OS Command (OS Command Injection')23-Feb-2023 2.3-Feb-20237.8A subsect CLI validation of argument of an affected command. A successful exploit could allow the attacker to execute argument of an affected command. A successful exploit could allow the attacker to execute argument of an affected command. A successful exploit could allow the attacker to execute argument of an affected command. A successful exploit could allow the attacker to execute argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.0-CIS-NX-O- 170323/1110Affected Version(s): 15.2\\(1g\)Up to VE-2023- 200500-CIS-NX-O- 170323/1110	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Version(s): * Up to (excluding) 9.3\(10\)Affected Version(s): * Up to (excluding) 9.3\(10\)A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability is due to insufficient vulnerability is due to special Elements used in an Injection')0-CIS-NX-0- 170323/111023-Feb-20237.87.8affected command. A successful exploit could allow the attacker to execute argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.0-CIS-NX-0- 170323/1110				the currently logged-						
Improper Neutralizat ion of Special Elements used in an DS Command Injection')23-Feb-20237.8A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system operating systemhttps://sec.clo udaps.cisco.c udaps.cisco.c enter/content /CiscoSecurity/ divisory/cisc orsa-nxos-cli- euQVK9u0-CIS-NX-0- 170323/11100-CIS-NX-0- 170323/										
Improper Neutralizat ion of Special Elements used in an nof Special Command Injection')23-Feb-20237.87.8CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.https://sec.clo udaps.cisco.c om/security/c enter/content (CiscoScurity) o-CIS-NX-0- 170323/11100-CIS-NX-0- 170323/11100-CIS-NX-0 170323/11107.87.860-CIS-NX-0- 170323/11100-CIS-NX-0- (CiscoScurity) could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user.0-CIS-NX-0- 170323/1110	Affected Ver	Affected Version(s): * Up to (excluding) 9.3\\(10\\)								
	Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')			CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged- in user. CVE ID : CVE-2023-	udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxos-cli- cmdinject-					

0-1

1-2

2-3

3-4 4-5 Page **695** of **859** 5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	0-CIS-NX-0- 170323/1111

0-1

1-2

2-3

3-4 4-5 Page **696** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023-		
			20089		
Affected Ver	<mark>sion(s): 15.2\\(</mark>	2e\\)	A vulnerability in the		
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	O-CIS-NX-O- 170323/1112

0-1

1-2

2-3 3-4 4-5 Page 697 of 859 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Affected Ver	sion(s): 15.2\\(2f\\)			
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	0-CIS-NX-0- 170323/1113

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which could result in		
			an unexpected		
			reload of the device.		
			This vulnerability is		
			due to incorrect		
			error checking when		
			parsing ingress LLDP		
			packets. An attacker		
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly		
			reloads. Note: This		
			vulnerability cannot		
			be exploited by		
			transit traffic		
			through the device.		
			The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		
			the affected device		
			(Layer 2 adjacent). In		
			addition, the attack		
			surface for this		
			vulnerability can be		
			reduced by disabling		
			LLDP on interfaces		
			where it is not		
			required.		
			-		

0-1

1-2

2-3 3-4 4-5 Page 699 of 859 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2023- 20089					
Affected Ver	Affected Version(s): 15.2\\(2g\\)							
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device.	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	0-CIS-NX-0- 170323/1114			

0-1

1-2

2-3

3-4 4-5 Page **700** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required.		
			CVE ID : CVE-2023- 20089		
Affected Ver	sion(s): 15.2\\(2h\\)			
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	0-CIS-NX-0- 170323/1115

0-1

1-2

2-3 3-4 4-5 Page **701** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Affected Ver	sion(s): 15.2\\([3e\\]	20007		
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI)	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp-	O-CIS-NX-O- 170323/1116

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mode could allow an unauthenticated,	dos- ySCNZOpX	
			adjacent attacker to	yschzopz	
			cause a memory leak,		
			which could result in		
			an unexpected		
			reload of the device.		
			This vulnerability is		
			due to incorrect		
			error checking when		
			parsing ingress LLDP		
			packets. An attacker		
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly reloads. Note: This		
			vulnerability cannot		
			be exploited by		
			transit traffic		
			through the device.		
			The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		
			the affected device		
			(Layer 2 adjacent). In		
			addition, the attack		
			surface for this		
			vulnerability can be		

0-1

1-2

2-3 3-4 4-5 Page **703** of **859** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023-		
			20089		
Affected Ver	sion(s): 15.2\\(3f\\)	-	-	
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	0-CIS-NX-0- 170323/1117

0-1

1-2

2-3

3-4 4-5 Page **704** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023-		
Affected Ver	sion(s): 15.2\\(3g\\)	20089		
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	O-CIS-NX-O- 170323/1118

0-1

1-2

2-33-44-5Page 705 of 859

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required.	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20089		
Affected Ver	sion(s): 15.2\\(4d\\)		I	·
Missing Release of Memory after	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco	https://sec.clo udapps.cisco.c om/security/c enter/content	0-CIS-NX-0- 170323/1119

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective			Nexus 9000 Series	/CiscoSecurity	
Lifetime			Fabric Switches in	Advisory/cisc	
			Application Centric	o-sa-aci-lldp-	
			Infrastructure (ACI)	dos-	
			Mode could allow an	ySCNZOpX	
			unauthenticated,		
			adjacent attacker to		
			cause a memory leak,		
			which could result in		
			an unexpected		
			reload of the device.		
			This vulnerability is		
			due to incorrect		
			error checking when		
			parsing ingress LLDP		
			packets. An attacker		
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly		
			reloads. Note: This		
			vulnerability cannot		
			be exploited by		
			transit traffic		
			through the device.		
			The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		
			the affected device		

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Affected Ver	sion(s): 15.2\\([4e\\)			
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	O-CIS-NX-O- 170323/1120

0-1

1-2

2-3

3-4 4-5 Page **708** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Affected Ver	sion(s): 15.2\\(4f\\)	L		I
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	O-CIS-NX-O- 170323/1121

0-1

1-2

2-3

3-4 4-5 Page **709** of **859** 6-7 7-8

Weakness Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness Publish Date Image: Construction of the second of the	CVSSv3	due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this	Patch	NCIIPC ID
Affected Version(s): 15.2	\(5c\\)	reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Allected version(S): 15.2				

0-1

1-2

2-3

3-4 4-5 Page **710** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	O-CIS-NX-O- 170323/1122

0-1

1-2

2-3

3-4 4-5 Page **711** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023-		
			20089		
Affected Ver	sion(s): 15.2\\(5d\\)			
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	0-CIS-NX-0- 170323/1123

0-1

1-2

2-33-44-5Page 712 of 859

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. CVE ID : CVE-2023- 20089		
Affected Ver	sion(s): 15.2\\(5e\\)			
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	O-CIS-NX-O- 170323/1124

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which could result in		
			an unexpected		
			reload of the device.		
			This vulnerability is		
			due to incorrect		
			error checking when		
			parsing ingress LLDP		
			packets. An attacker		
			could exploit this		
			vulnerability by		
			sending a steady		
			stream of crafted		
			LLDP packets to an		
			affected device. A		
			successful exploit		
			could allow the		
			attacker to cause a		
			memory leak, which		
			could result in a		
			denial of service		
			(DoS) condition		
			when the device		
			unexpectedly		
			reloads. Note: This		
			vulnerability cannot		
			be exploited by		
			transit traffic		
			through the device.		
			The crafted LLDP		
			packet must be		
			targeted to a directly		
			connected interface,		
			and the attacker		
			must be in the same		
			broadcast domain as		
			the affected device		
			(Layer 2 adjacent). In		
			addition, the attack		
			surface for this		
			vulnerability can be		
			reduced by disabling		
			LLDP on interfaces		
			where it is not		
			required.		

0-1

1-2

2-3

3-4 4-5 Page **714** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			CVE ID : CVE-2023- 20089				
Affected Ver	Affected Version(s): 16.0\\(1g\\)						
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device.	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	0-CIS-NX-0- 170323/1125		

0-1

1-2

2-3

3-4 4-5 Page **715** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required.		
			CVE ID : CVE-2023- 20089		
Affected Ver	sion(s): 16.0\\(1j\\)			
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-aci-lldp- dos- ySCNZOpX	0-CIS-NX-0- 170323/1126

0-1

1-2

2-3 3-4 4-5 Page **716** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	D	escriptio	n & CVE I	D		Patch			NCIIP	C ID
			LLL affe suc cou att me cou den (Do wh und rel vul be tra thr The pao tar con and thr Cou cu vul be tra thr The pao tar cou cu vul be tra thr Cou cu vul be tra thr Cou cu vul be tra thr Cou vul be tra thr Cou vul be tra thr Cou vul be tra thr Cou vul be tra thr Cou vul be tra thr Cou vul be tra thr Cou vul be tra thr Cou vul be tra thr Cou vul be tra thr Cou vul be tra thr Cou vul be tra thr Cou vul be tra thr Cou cou thr Cou vul be tra thr Cou cou thr Cou vul be tra thr Cou thr thr Cou th	DP packa ected de ccessful ild allow acker to mory le ild resul nial of se oS) cond en the d expected oads. No nerabili exploite nsit traf ough the e crafted cket mus geted to nected d the att st be in oadcast o e affected yer 2 ac dition, the face for nerabili luced by DP on in ere it is juired.	ets to an vice. A exploit v the cause a ak, whice it in a ervice lition levice dly ote: This ty canno ed by fic e device d LLDP st be a direct interfac acker the sam domain d device this ty can b v disablin terfaces	n ch ot ch ly e, as as i. In k ne ng 5						
				089								
	s_6200_firmwa	ire										
Affected Vers	sion(s): -			1 .		, ,	1 .	. ,	1			
Improper Neutralizat ion of Special Elements used in an OS	23-Feb-2023	6.7	CLI Fir Ser Fir Sec	l of Cisco epower ries, Cisc epower curity Ap	4100 co	es,	uda om, ent /Cis Adv	os://se pps.cis /securi er/cont scoSecu visory/c a-nxfp-	co.c ty/c tent ırity		IS-UC 323/	S 1127
CVSS Scoring S		1_2)_2	2 /	ΛΕ		6	6.7	7.0		8.0	0.10
CVSS Scoring S	Scale 0-1	1-2	2-3	3-4	4-5	5-	6	6-7	7-8	5	8-9	9-10

Page **717** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015	cmdinj- XXBZjtR	
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software	https://sec.clo udapps.cisco.c om/security/c enter/content	O-CIS-UCS 170323/1128

0-1

1-2

2-33-44-5Page 718 of 859

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and in the	/CiscoSecurity	
			configuration export	Advisory/cisc	
			feature of Cisco FXOS	o-sa-ucsm-	
			Software could allow	bkpsky-	
			an unauthenticated	H8FCQgsA	
			attacker with access		
			to a backup file to		
			decrypt sensitive		
			information stored in		
			the full state and		
			configuration backup		
			files. This		
			vulnerability is due		
			to a weakness in the		
			encryption method		
			used for the backup		
			function. An attacker		
			could exploit this		
			vulnerability by		
			leveraging a static		
			key used for the		
			backup configuration		
			feature. A successful		
			exploit could allow		
			the attacker to		
			decrypt sensitive		
			information that is		
			stored in full state		
			and configuration		
			backup files, such as		
			local user		
			credentials,		
			authentication		
			server passwords,		
			Simple Network		
			Management		
			Protocol (SNMP)		
			community names,		
			and other		
			credentials.		
			CVE ID : CVE-2023-		
			20016		
Product: uc	s_6248up_firm	ware			

0-1

1-2

2-3

3-4 4-5 Page **719** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): -	L			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	O-CIS-UCS 170323/1129

0-1

1-2

2-33-44-5Page 720 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	0-CIS-UCS 170323/1130

0-1

1-2

2-3 3-4 4-5 Page **721** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Protocol (SNMP) community names, and other credentials.		
			CVE ID : CVE-2023- 20016		
Product: uc	s_6296up_firm	ware			
Affected Ver	sion(s): -		-	-	_
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	0-CIS-UCS 170323/1131

0-1

1-2

2-3

3-4 4-5 Page **722** of **859** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	0-CIS-UCS 170323/1132

0-1

1-2

2-3

3-4 4-5 Page **723** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Product: uc	s_6300_firmwa	are	20010		
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	0-CIS-UCS 170323/1133

0-1

1-2

2-3

3-4 4-5 Page **724** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	O-CIS-UCS 170323/1134

0-1

1-2

2-3

3-4 4-5 Page **725** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
	s_6324_firmwa	are	l		l
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	0-CIS-UCS 170323/1135

0-1

1-2

2-3

3-4 4-5 Page **726** of **859** 5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges.		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	20015 A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	0-CIS-UCS 170323/1136

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Product: ucs	5_6332-16up_f	irmware			
Affected Vers	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	0-CIS-UCS 170323/1137
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 728 of 859					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm-	0-CIS-UCS 170323/1138

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Weakness	Publish Date	CVSSv3	Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023-	Patch bkpsky- H8FCQgsA			
Product: ucs_6332_firmware							
-	Affected Version(s): -						

0-1

1-2

2-3

3-4 4-5 Page **730** of **859** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges.	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	0-CIS-UCS 170323/1139

0-1

1-2

2-3

3-4 4-5 Page **731** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names,	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	0-CIS-UCS 170323/1140

0-1

1-2

2-3

3-4 4-5 Page **732** of **859** 5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and other credentials. CVE ID : CVE-2023- 20016		
Product: uc	s_64108_firmv	vare		L	
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	O-CIS-UCS 170323/1141

0-1

1-2

2-3

3-4 4-5 Page **733** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges.		
			CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	0-CIS-UCS 170323/1142

0-1

1-2

2-3

3-4 4-5 Page **734** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Improper Authentica tion	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300- FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-elyfex- dos-gfvcByx	0-CIS-UCS 170323/1143

0-1

1-2

2-3

3-4 4-5 Page **735** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. CVE ID : CVE-2023-		
Product: uc	<mark>s_6454_firmwa</mark>	ro	20012		
Affected Ver					
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	0-CIS-UCS 170323/1144

0-1

1-2

2-3

3-4 4-5 Page **736** of **859** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges.		
			CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	0-CIS-UCS 170323/1145

0-1

1-2

2-3

3-4 4-5 Page **737** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023-		
Improper Authentica tion	23-Feb-2023	4.6	20016 A vulnerability in the CLI console login authentication of Cisco Nexus 9300- FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-elyfex- dos-gfvcByx	0-CIS-UCS 170323/1146

0-1

1-2

2-33-44-5Page 738 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. CVE ID : CVE-2023-		
Productive	s_6536_firmwa	ro	20012		
Affected Ver					
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-nxfp- cmdinj- XXBZjtR	0-CIS-UCS 170323/1147

0-1

1-2

2-3

3-4 4-5 Page **739** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. CVE ID : CVE-2023- 20015		
Use of Insufficient ly Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-ucsm- bkpsky- H8FCQgsA	O-CIS-UCS 170323/1148

0-1

1-2

2-3

3-4 4-5 Page **740** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. CVE ID : CVE-2023- 20016		
Improper Authentica tion	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300- FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by	https://sec.clo udapps.cisco.c om/security/c enter/content /CiscoSecurity Advisory/cisc o-sa-elyfex- dos-gfvcByx	0-CIS-UCS 170323/1149

0-1

1-2

2-3 3-4 4-5 Page **741** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. CVE ID : CVE-2023-						
Vendor: Del	hian		20012						
	Product: debian_linux								
Affected Ver	sion(s): 10.0								
N/A	22-Feb-2023	8.8	The mono package before 6.8.0.105+dfsg-3.3 for Debian allows arbitrary code execution because the application/x- ms-dos-executable MIME type is associated with an un-sandboxed Mono CLR interpreter. CVE ID : CVE-2023-	N/A	O-DEB-DEBI- 170323/1150				
Allocation of Resources Without Limits or Throttling	23-Feb-2023	7.5	An allocation of resources without limits or throttling vulnerability exists in curl <v7.88.0 based on the "chained" HTTP compression algorithms, meaning</v7.88.0 	https://securi ty.netapp.com /advisory/nta p-20230309- 0006/	O-DEB-DEBI- 170323/1151				

0-1

1-2

2-3

3-4 4-5 Page **742** of **859** 6-7 7-

5-6

8 8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that a server response can be compressed multiple times and potentially with differentalgorithms. The number of acceptable "links" in this "decompression chain" wascapped, but the cap was implemented on a per-header basis allowing a maliciousserver to insert a virtually unlimited number of compression steps simply byusing many headers. The use of such a decompression chain could result in a "malloc bomb", making curl end up spending enormous amounts of allocated heap memory, or trying to and returning out of memory errors. CVE ID : CVE-2023- 23916		
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running	https://nodej s.org/en/blog /vulnerability /february- 2023- security- releases/	O-DEB-DEBI- 170323/1152

0-1

1-2

2-3

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with elevated privileges. CVE ID : CVE-2023- 23920		
Affected Ver	sion(s): 11.0		23720		
N/A	28-Feb-2023	9.8	SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because serialization is mishandled. The fixed versions are 3.2.18, 4.0.10, 4.1.8, and 4.2.1. CVE ID : CVE-2023- 27372	https://git.spi p.net/spip/spi p/commit/5a edf49b89415a 4df3eb775eee 3801a2b4b88 266, https://git.spi p.net/spip/spi p/commit/96f beb38711c67 06e62457f2b 732a652a04a 409d	O-DEB-DEBI- 170323/1153
Allocation of Resources Without Limits or Throttling	23-Feb-2023	7.5	An allocation of resources without limits or throttling vulnerability exists in curl <v7.88.0 based on the "chained" HTTP compression algorithms, meaning that a server response can be compressed multiple times and potentially with differentalgorithms. The number of acceptable "links" in this "decompression chain" wascapped, but the cap was implemented on a per-header basis allowing a maliciousserver to</v7.88.0 	https://securi ty.netapp.com /advisory/nta p-20230309- 0006/	O-DEB-DEBI- 170323/1154

0-1

1-2

2-3

3-4 4-5 Page **744** of **859** 5-6

9-10

	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insert a virtually unlimited number of compression steps simply byusing many headers. The use of such a decompression chain could result in a "malloc bomb", making curl end up spending enormous amounts of allocated heap memory, or trying to and returning out of memory errors. CVE ID : CVE-2023- 23916		
Uncontroll ed Resource Consumpti on	21-Feb-2023	6.5	Libreswan 4.9 allows remote attackers to cause a denial of service (assert failure and daemon restart) via crafted TS payload with an incorrect selector length. CVE ID : CVE-2023-	https://github .com/libreswa n/libreswan/i ssues/954	O-DEB-DEBI- 170323/1155
Vendor: Dell	1		23009		
	000_firmware				
	sion(s): 9.0.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for-	O-DEL-A200- 170323/1156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	multiple- security	
Affected Vers	sion(s): 9.1.0.0				l
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-A200- 170323/1157
Affected Vers	sion(s): 9.2.0.0				1
Uncontroll ed	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000,	https://www. dell.com/supp	O-DEL-A200- 170323/1158
CVSS Scoring S	icale 0-1	1-2 2	-3 3-4 4-5 5 Page 746 of 859	-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource Consumpti on			H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	
Affected Ver	sion(s): 9.2.1.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-A200- 170323/1159

0-1

1-2

2-3 3-4 4-5 Page **747** of **859** 5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mechanism causing a denial of service. CVE ID : CVE-2023- 23689		
Affected Ver	sion(s): 9.3.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-A200- 170323/1160
Affected Ver	sion(s): 9.4.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-A200- 170323/1161

0-1

1-2

2-3 3-4 4-5 Page **748** of **859** 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689					
Affected Vers	sion(s): 9.5.0.0		L		I			
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-A200- 170323/1162			
-	Product: a200_firmware							
Affected Vers	sion(s): 9.0.0.0				-			
Uncontroll ed Resource	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600,	https://www. dell.com/supp ort/kbdoc/en-	0-DEL-A200- 170323/1163			
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3 3-4 4-5 5</mark> Page 749 of 859	-6 6-7 7-8	8 8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumpti on			H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	
Affected Ver	sion(s): 9.1.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-A200- 170323/1164

0-1

1-2

2-33-44-5Page 750 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mechanism causing a denial of service. CVE ID : CVE-2023-		
			23689		
Affected Ver	sion(s): 9.2.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-A200- 170323/1165
Affected Ver	sion(s): 9.2.1.0		<u></u>	1	I
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-A200- 170323/1166

0-1

1-2

2-3 3-4 4-5 Page **751** of **859** 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689		
Affected Ver	sion(s): 9.3.0.0		23003		
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-A200- 170323/1167
Affected Ver	sion(s): 9.4.0.0		NND C :		
Uncontroll ed Resource	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810	https://www. dell.com/supp ort/kbdoc/en- us/00020989	O-DEL-A200- 170323/1168

3-4

Page 752 of 859

4-5

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumpti on			integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	
Affected Ver	sion(s): 9.5.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-A200- 170323/1169

0-1

1-2

2-3

3-4 4-5 Page **753** of **859** 5-6

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23689		
Product: em	ic_powerscale_	onefs			
Affected Vers	sion(s): From (i	ncluding)	9.4.0.0 Up to (including) 9.4.0.11	
Incorrect Default Permission s	28-Feb-2023	7.1	Dell PowerScale OneFS 9.4.0.x contains an incorrect default permissions vulnerability. A local malicious user could potentially exploit this vulnerability to overwrite arbitrary files causing denial of service. CVE ID : CVE-2023- 25540	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-EMC 170323/1170
Product: f80	00_firmware				<u> </u>
Affected Ver	sion(s): 9.0.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-F800- 170323/1171

0-1

1-2

2-3 3-4 4-5 Page **754** of **859** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23689		
Affected Ver	sion(s): 9.1.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-F800- 170323/1172
Affected Ver	sion(s): 9.2.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-F800- 170323/1173

0-1

1-2

2-33-44-5Page 755 of 859

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023-		
Affected Ver	sion(s): 9.2.1.0		23689		
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-F800- 170323/1174
Affected Ver	sion(s): 9.3.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale-	O-DEL-F800- 170323/1175

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	onefs- security- updates-for- multiple- security	
			CVE ID : CVE-2023- 23689		
Affected Ver	sion(s): 9.4.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-F800- 170323/1176

0-1

1-2

2-3

3-4 4-5 Page **757** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23689		
Affected Ver	sion(s): 9.5.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-F800- 170323/1177
Product: f8	10_firmware				
Affected Ver	sion(s): 9.0.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-F810- 170323/1178

0-1

1-2

2-33-44-5Page 758 of 859

5-6 6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689		
Affected Ver	sion(s): 9.1.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-F810- 170323/1179
	sion(s): 9.2.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc-	O-DEL-F810- 170323/1180
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5	<mark>-6 6-7 7-</mark> 8	8 8-9 9-10

Page **759** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	powerscale- onefs- security- updates-for- multiple- security	
Affected Ver Uncontroll ed Resource Consumpti on	sion(s): 9.2.1.0 28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-F810- 170323/1181

0-1

1-2

2-3

3-4 4-5 Page **760** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23689		
Affected Ver	sion(s): 9.3.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-F810- 170323/1182
Affected Ver	sion(s): 9.4.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-F810- 170323/1183

0-1

1-2

2-3 3-4 4-5 Page **761** of **859** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689		
Affected Vers	sion(s): 9.5.0.0		23009		
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-F810- 170323/1184
Product: h4	00_firmware				
Affected Vers	sion(s): 9.0.0.0				
Uncontroll ed Resource	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc-	O-DEL-H400- 170323/1185
	Scale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumpti on			management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	powerscale- onefs- security- updates-for- multiple- security	
Affected Vers Uncontroll ed Resource Consumpti on	sion(s): 9.1.0.0 28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H400- 170323/1186

0-1

1-2

2-3

3-4 4-5 Page **763** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23689		
Affected Ver	sion(s): 9.2.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H400- 170323/1187
Affected Ver	sion(s): 9.2.1.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H400- 170323/1188

0-1

1-2

2-3 3-4 4-5 Page **764** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023-		
Affected Mer	sion(s): 9.3.0.0		23689		
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H400- 170323/1189
Affected Ver	sion(s): 9.4.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale-	O-DEL-H400- 170323/1190

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	onefs- security- updates-for- multiple- security	
			CVE ID : CVE-2023- 23689		
Affected Ver	sion(s): 9.5.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H400- 170323/1191

0-1

1-2

2-3

3-4 4-5 Page **766** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23689		
Product: h5	00_firmware				
Affected Ver	sion(s): 9.0.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H500- 170323/1192
Affected Ver	sion(s): 9.1.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H500- 170323/1193

0-1

1-2

2-3

3-4 4-5 Page **767** of **859** 5-6 6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689		
Affected Ver	sion(s): 9.2.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H500- 170323/1194
	sion(s): 9.2.1.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc-	O-DEL-H500- 170323/1195
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5	<mark>-6 6-7 7-</mark> 8	8 8-9 9-10

Page **768** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	powerscale- onefs- security- updates-for- multiple- security	
Affected Ver Uncontroll ed Resource Consumpti on	sion(s): 9.3.0.0 28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H500- 170323/1196

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23689		
Affected Ver	sion(s): 9.4.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H500- 170323/1197
Affected Ver	sion(s): 9.5.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H500- 170323/1198

0-1

1-2

2-3 3-4 4-5 Page **770** of **859** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.						
			CVE ID : CVE-2023- 23689						
	600_firmware								
Affected Ver	sion(s): 9.0.0.0								
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H560- 170323/1199				
Affected Ver	Affected Version(s): 9.1.0.0								
Uncontroll ed Resource	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc-	O-DEL-H560- 170323/1200				
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	8 8-9 9-10				

Page **771** of **859**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumpti on			management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	powerscale- onefs- security- updates-for- multiple- security	
Uncontroll ed Resource Consumpti on	sion(s): 9.2.0.0 28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H560- 170323/1201

0-1

1-2

2-3

3-4 4-5 Page **772** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23689		
Affected Ver	sion(s): 9.2.1.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H560- 170323/1202
Affected Ver	sion(s): 9.3.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H560- 170323/1203

0-1

1-2

2-3 3-4 4-5 Page **773** of **859** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023-		
Affected Ver	sion(s): 9.4.0.0		23689		
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H560- 170323/1204
Affected Ver	sion(s): 9.5.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale-	O-DEL-H560- 170323/1205

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	onefs- security- updates-for- multiple- security	
	00_firmware				
Affected Ver	sion(s): 9.0.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H600- 170323/1206

0-1

1-2

2-3

3-4 4-5 Page **775** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23689		
Affected Ver	sion(s): 9.1.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H600- 170323/1207
Affected Ver	sion(s): 9.2.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H600- 170323/1208

0-1

1-2

2-3 3-4 4-5 Page **776** of **859** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023-		
Affected Ver	sion(s): 9.2.1.0		23689		
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H600- 170323/1209
Affected Ver	sion(s): 9.3.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale-	O-DEL-H600- 170323/1210

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	onefs- security- updates-for- multiple- security	
			CVE ID : CVE-2023- 23689		
Affected Ver	sion(s): 9.4.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H600- 170323/1211

0-1

1-2

2-3 3-4 4-5 Page **778** of **859** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23689		
Affected Vers	sion(s): 9.5.0.0				
Uncontroll ed Resource Consumpti on	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. CVE ID : CVE-2023- 23689	https://www. dell.com/supp ort/kbdoc/en- us/00020989 5/dell-emc- powerscale- onefs- security- updates-for- multiple- security	O-DEL-H600- 170323/1212
Vendor: Dra	ytek				
Product: vig	or2960_firmw	vare			
Affected Vers	sion(s): 1.5.1.4				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Feb-2023	5.5	A vulnerability classified as problematic has been found in DrayTek Vigor 2960 1.5.1.4. Affected is the function sub_1DF14 of the file /cgi- bin/mainfunction.cgi . The manipulation of the argument option	N/A	0-DRA-VIGO- 170323/1213
CVSS Scoring S	Scale 0-1	1-2 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
			with the input //etc/password leads to path traversal. The attack needs to be done within the local network. The exploit has been disclosed to the public and may be used. VDB- 221742 is the identifier assigned to this vulnerability.		
			CVE ID : CVE-2023- 1009		
Vendor: Fed	loraproject			<u> </u>	
Product: fee	lora				
Affected Ver	sion(s): 36				
Allocation of Resources Without Limits or Throttling	23-Feb-2023	7.5	An allocation of resources without limits or throttling vulnerability exists in curl <v7.88.0 based on the "chained" HTTP compression algorithms, meaning that a server response can be compressed multiple times and potentially with differentalgorithms. The number of acceptable "links" in this "decompression chain" wascapped, but the cap was implemented on a per-header basis allowing a maliciousserver to</v7.88.0 	https://securi ty.netapp.com /advisory/nta p-20230309- 0006/	O-FED-FEDO- 170323/1214

0-1

1-2

2-33-44-5Page 780 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insert a virtually unlimited number of compression steps simply byusing many headers. The use of such a decompression chain could result in a "malloc bomb", making curl end up spending enormous amounts of allocated heap memory, or trying to and returning out of memory errors. CVE ID : CVE-2023- 23916		
Improper Certificate Validation	27-Feb-2023	5.5	A flaw was found in RHDS 11 and RHDS 12. While browsing entries LDAP tries to decode the userPassword attribute instead of the userCertificate attribute which could lead into sensitive information leaked. An attacker with a local account where the cockpit- 389-ds is running can list the processes and display the hashed passwords. The highest threat from this vulnerability is to data confidentiality. CVE ID : CVE-2023- 1055	https://bugzil la.redhat.com /show_bug.cgi ?id=2173517 #c0	O-FED-FEDO- 170323/1215

0-1

1-2

2-3

3-4 4-5 Page **781** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 37				
Exposure of Resource to Wrong Sphere	20-Feb-2023	7.5	In Epiphany (aka GNOME Web) through 43.0, untrusted web content can trick users into exfiltrating passwords, because autofill occurs in sandboxed contexts.	https://gitlab. gnome.org/G NOME/epipha ny/- /merge_reque sts/1275	O-FED-FEDO- 170323/1216
			CVE ID : CVE-2023- 26081		
Double Free	28-Feb-2023	7.2	Sudo before 1.9.13p2 has a double free in the per-command chroot feature.	N/A	O-FED-FEDO- 170323/1217
			CVE ID : CVE-2023- 27320		
Improper Certificate Validation	27-Feb-2023	5.5	A flaw was found in RHDS 11 and RHDS 12. While browsing entries LDAP tries to decode the userPassword attribute instead of the userCertificate attribute which could lead into sensitive information leaked. An attacker with a local account where the cockpit- 389-ds is running can list the processes and display the hashed passwords. The highest threat from this vulnerability is to data confidentiality.	https://bugzil la.redhat.com /show_bug.cgi ?id=2173517 #c0	0-FED-FEDO- 170323/1218

0-1

1-2

2-33-44-5Page 782 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 1055		
Vendor: Go	ogle				
Product: an	droid				
Affected Ver	sion(s): -				
Use After Free	22-Feb-2023	8.8	Use after free in Web Payments API in Google Chrome on Android prior to 110.0.5481.177 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) CVE ID : CVE-2023- 0927	https://chrom ereleases.goog leblog.com/20 23/02/stable- channel- desktop- update_22.ht ml	O-GOO-ANDR- 170323/1219
Use After Free	28-Feb-2023	7.8	In several functions of the Android Linux kernel, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 257443051Referenc es: Upstream kernel	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1220

0-1

1-2

2-33-44-5Page 783 of 859

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20937		
Use After Free	28-Feb-2023	7.8	In binder_transaction_b uffer_release of binder.c, there is a possible use after free due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 257685302Referenc es: Upstream kernel CVE ID : CVE-2023- 20938	https://sourc e.android.com /security/bull etin/2023-02- 01	0-G00-ANDR- 170323/1221
Affected Ver	sion(s): 10.0	L			
Use After Free	28-Feb-2023	7.8	In several functions of MediaCodec.cpp, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-12L	https://sourc e.android.com /security/bull etin/2023-02- 01	0-G00-ANDR- 170323/1222

0-1

1-2

2-3 3-4 4-5 Page **784** of **859** 5-6

7-8

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-245860753 CVE ID : CVE-2023- 20933		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Feb-2023	7.8	In clearApplicationUser Data of ActivityManagerServ ice.java, there is a possible way to remove system files due to a path traversal error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-240267890 CVE ID : CVE-2023- 20943	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1223
Deserializa tion of Untrusted Data	28-Feb-2023	7.8	In run of ChooseTypeAndAcco untActivity.java, there is a possible escalation of privilege due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is	https://sourc e.android.com /security/bull etin/2023-02- 01	O-GOO-ANDR- 170323/1224

0-1

1-2

3-4 4-5 2-3 Page 785 of 859

7-8

6-7

5-6

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-244154558 CVE ID : CVE-2023- 20944		
Out-of- bounds Write	28-Feb-2023	7.8	In phNciNfc_MfCreateX chgDataHdr of phNxpExtns_MifareS td.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-246932269 CVE ID : CVE-2023- 20945	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1225
Improper Input Validation	28-Feb-2023	3.3	In onCreatePreferences of EditInfoFragment.jav a, there is a possible way to read contacts belonging to other users due to improper input validation. This could lead to local	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1226

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-12L Android-12L Android-13Android ID: A-248251018 CVE ID : CVE-2023- 20932		
Affected Ver	sion(s): 11.0				
N/A	28-Feb-2023	9.8	In onStart of BluetoothSwitchPref erenceController.jav a, there is a possible permission bypass due to a confused deputy. This could lead to remote escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android- 12 Android-12L Android-13Android ID: A-244423101 CVE ID : CVE-2023- 20946	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1227
Use After Free	28-Feb-2023	7.8	In several functions of MediaCodec.cpp,	https://sourc e.android.com	0-GOO-ANDR- 170323/1228

0-1

1-2

2-3 3-4 4-5 Page **787** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-245860753 CVE ID : CVE-2023- 20933	/security/bull etin/2023-02- 01	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Feb-2023	7.8	In clearApplicationUser Data of ActivityManagerServ ice.java, there is a possible way to remove system files due to a path traversal error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-13Android ID: A-240267890	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1229

0-1

1-2

2-3

3-4 4-5 Page **788** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20943		
Deserializa tion of Untrusted Data	28-Feb-2023	7.8	In run of ChooseTypeAndAcco untActivity.java, there is a possible escalation of privilege due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-244154558 CVE ID : CVE-2023- 20944	https://sourc e.android.com /security/bull etin/2023-02- 01	0-G00-ANDR- 170323/1230
Improper Input Validation	28-Feb-2023	3.3	In onCreatePreferences of EditInfoFragment.jav a, there is a possible way to read contacts belonging to other users due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://sourc e.android.com /security/bull etin/2023-02- 01	0-G00-ANDR- 170323/1231

0-1

1-2

2-3

3-4 4-5 Page **789** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-248251018		
			CVE ID : CVE-2023- 20932		
Affected Ver	sion(s): 12.0				
N/A	28-Feb-2023	9.8	In onStart of BluetoothSwitchPref erenceController.jav a, there is a possible permission bypass due to a confused deputy. This could lead to remote escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android- 12 Android-12L Android-13Android ID: A-244423101 CVE ID : CVE-2023-	https://sourc e.android.com /security/bull etin/2023-02- 01	0-G00-ANDR- 170323/1232
Use After Free	28-Feb-2023	7.8	20946 In several functions of MediaCodec.cpp, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of	https://sourc e.android.com /security/bull etin/2023-02- 01	0-G00-ANDR- 170323/1233

0-1

1-2

2-3 3-4 4-5 Page **790** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-245860753 CVE ID : CVE-2023- 20933		
N/A	28-Feb-2023	7.8	In resolveAttributionSo urce of ServiceUtilities.cpp, there is a possible way to disable the microphone privacy indicator due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android- 12L Android- 13Android ID: A- 258672042 CVE ID : CVE-2023-	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1234
Improper Locking	28-Feb-2023	7.8	20934 In multiple functions of looper_backed_event _loop.cpp, there is a possible way to	https://sourc e.android.com /security/bull	0-GOO-ANDR- 170323/1235

0-1

1-2

2-3

3-4 4-5 Page **791** of **859** 8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corrupt memory due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android- 12L Android- 13Android ID: A- 243362981 CVE ID : CVE-2023- 20939	etin/2023-02- 01	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Feb-2023	7.8	In clearApplicationUser Data of ActivityManagerServ ice.java, there is a possible way to remove system files due to a path traversal error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-240267890 CVE ID : CVE-2023- 20943	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1236

0-1

1-2

2-3

3-4 4-5 Page **792** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserializa tion of Untrusted Data	28-Feb-2023	7.8	In run of ChooseTypeAndAcco untActivity.java, there is a possible escalation of privilege due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-244154558 CVE ID : CVE-2023- 20944	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1237
Out-of- bounds Read	28-Feb-2023	7.5	In dropFramesUntillfra me of AAVCAssembler.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android- 12L Android-	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1238

0-1

1-2

2-3 3-4 4-5 Page **793** of **859** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13Android ID: A- 230630526 CVE ID : CVE-2023- 20948		
Improper Input Validation	28-Feb-2023	3.3	In onCreatePreferences of EditInfoFragment.jav a, there is a possible way to read contacts belonging to other users due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-248251018 CVE ID : CVE-2023- 20932	https://sourc e.android.com /security/bull etin/2023-02- 01	0-G00-ANDR- 170323/1239
Affected Ver	sion(s): 12.1				
N/A	28-Feb-2023	9.8	In onStart of BluetoothSwitchPref erenceController.jav a, there is a possible permission bypass due to a confused deputy. This could lead to remote escalation of privilege in Bluetooth settings	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1240

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android- 12 Android-12L Android-13Android ID: A-244423101 CVE ID : CVE-2023- 20946		
Use After Free	28-Feb-2023	7.8	In several functions of MediaCodec.cpp, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-245860753 CVE ID : CVE-2023- 20933	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1241
N/A	28-Feb-2023	7.8	In resolveAttributionSo urce of ServiceUtilities.cpp, there is a possible way to disable the microphone privacy indicator due to a	https://sourc e.android.com /security/bull etin/2023-02- 01	0-G00-ANDR- 170323/1242

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android- 12L Android- 13Android ID: A- 258672042		
			CVE ID : CVE-2023- 20934		
Improper Locking	28-Feb-2023	7.8	In multiple functions of looper_backed_event _loop.cpp, there is a possible way to corrupt memory due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android- 12L Android- 13Android ID: A- 243362981 CVE ID : CVE-2023- 20939	https://sourc e.android.com /security/bull etin/2023-02- 01	0-G00-ANDR- 170323/1243
Improper Limitation of a Pathname to a	28-Feb-2023	7.8	In clearApplicationUser Data of ActivityManagerServ ice.java, there is a	https://sourc e.android.com /security/bull	0-GOO-ANDR- 170323/1244

0-1

1-2

2-3

3-4 4-5 Page **796** of **859** 8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			possible way to remove system files due to a path traversal error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-240267890 CVE ID : CVE-2023- 20943	etin/2023-02- 01	
Deserializa tion of Untrusted Data	28-Feb-2023	7.8	In run of ChooseTypeAndAcco untActivity.java, there is a possible escalation of privilege due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-244154558	https://sourc e.android.com /security/bull etin/2023-02- 01	O-GOO-ANDR- 170323/1245

0-1

1-2

2-3 3-4 4-5 Page **797** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20944		
Out-of- bounds Read	28-Feb-2023	7.5	In dropFramesUntilIfra me of AAVCAssembler.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android- 12L Android- 13Android ID: A- 230630526 CVE ID : CVE-2023- 20948	https://sourc e.android.com /security/bull etin/2023-02- 01	0-G00-ANDR- 170323/1246
Improper Input Validation	28-Feb-2023	3.3	In onCreatePreferences of EditInfoFragment.jav a, there is a possible way to read contacts belonging to other users due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1247

0-1

1-2

2-3

3-4 4-5 Page **798** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-248251018		
			CVE ID : CVE-2023- 20932		
Affected Ver	sion(s): 13.0				
N/A	28-Feb-2023	9.8	In onStart of BluetoothSwitchPref erenceController.jav a, there is a possible permission bypass due to a confused deputy. This could lead to remote escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: Android-11 Android- 12 Android-12L Android-13Android ID: A-244423101	https://sourc e.android.com /security/bull etin/2023-02- 01	0-G00-ANDR- 170323/1248
			CVE ID : CVE-2023- 20946		
Use After Free	28-Feb-2023	7.8	In several functions of MediaCodec.cpp, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1249

0-1

1-2

2-3

3-4 4-5 Page **799** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-245860753 CVE ID : CVE-2023- 20933		
N/A	28-Feb-2023	7.8	In resolveAttributionSo urce of ServiceUtilities.cpp, there is a possible way to disable the microphone privacy indicator due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android- 12L Android- 13Android ID: A- 258672042 CVE ID : CVE-2023- 20934	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1250
Improper Locking	28-Feb-2023	7.8	In multiple functions of looper_backed_event _loop.cpp, there is a possible way to corrupt memory due	https://sourc e.android.com /security/bull etin/2023-02- 01	O-GOO-ANDR- 170323/1251

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android- 12L Android- 13Android ID: A- 243362981		
			CVE ID : CVE-2023- 20939		
Improper Verificatio n of Cryptograp hic Signature	28-Feb-2023	7.8	In the Android operating system, there is a possible way to replace a boot partition due to improperly used crypto. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-256237041 CVE ID : CVE-2023- 20940	https://sourc e.android.com /security/bull etin/2023-02- 01	0-G00-ANDR- 170323/1252
Improper Limitation of a Pathname to a Restricted Directory	28-Feb-2023	7.8	In clearApplicationUser Data of ActivityManagerServ ice.java, there is a possible way to remove system files	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1253

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			due to a path traversal error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-240267890 CVE ID : CVE-2023-		
Deserializa tion of Untrusted Data	28-Feb-2023	7.8	20943 In run of ChooseTypeAndAcco untActivity.java, there is a possible escalation of privilege due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android- 11 Android-12 Android-12L Android-13Android ID: A-244154558 CVE ID : CVE-2023- 20944	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1254

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	28-Feb-2023	7.5	In dropFramesUntilIfra me of AAVCAssembler.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android- 12L Android- 13Android ID: A- 230630526 CVE ID : CVE-2023- 20948	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1255
Improper Input Validation	28-Feb-2023	3.3	In onCreatePreferences of EditInfoFragment.jav a, there is a possible way to read contacts belonging to other users due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: Android-10 Android-	https://sourc e.android.com /security/bull etin/2023-02- 01	0-GOO-ANDR- 170323/1256

0-1

1-2

2-3

3-4 4-5 Page **803** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11 Android-12 Android-12L Android-13Android ID: A-248251018		
			CVE ID : CVE-2023- 20932		
Vendor: H3	С				
Product: a2	10-g_firmware				
Affected Ver	sion(s): a210-gv	7100r005			
Improper Authentica tion	22-Feb-2023	9.8	An access control issue in H3C A210-G A210-GV100R005 allows attackers to authenticate without a password.	N/A	O-H3C-A210- 170323/1257
			CVE ID : CVE-2023- 24093		
Vendor: IBN	1				
Product: aix					
Affected Ver	sion(s): -				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Feb-2023	7.5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (//) to view arbitrary files on the system. IBM X-Force ID: 246333	https://www.i bm.com/supp ort/pages/no de/6953521, https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 46333	0-IBM-AIX- 170323/1258
Cleartext Storage of Sensitive	17-Feb-2023	5.5	CVE ID : CVE-2023- 24960 IBM InfoSphere Information Server 11.7 could allow a local user to obtain	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2	0-IBM-AIX- 170323/1259

0-1

1-2

2-3

3-4 4-5 Page **804** of **859** 6-7

5-6

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Informatio n			sensitive information from a log files. IBM X-Force ID: 246463. CVE ID : CVE-2023- 24964	46463, https://www.i bm.com/supp ort/pages/no de/6953519	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247646. CVE ID : CVE-2023- 25928	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 47646, https://www.i bm.com/supp ort/pages/no de/6956598	O-IBM-AIX- 170323/1260
Vendor: Kor	renix wave_2111l_fi	rmware			
	sion(s): * Up to		g) 1.6		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294	N/A	0-KOR-JETW- 170323/1261
Improper Neutralizat ion of	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series	N/A	O-KOR-JETW- 170323/1262

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Comman d Injection')			1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295		
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	O-KOR-JETW- 170323/1263
Product: jet	wave_2111_fir	mware	L	<u> </u>	
Affected Ver	sion(s): * Up to	(excluding	g) 1.5		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023-	N/A	O-KOR-JETW- 170323/1264
,,			23294		
Improper Neutralizat ion of Special Elements used in a	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via	N/A	O-KOR-JETW- 170323/1265

0-1

1-2

2-3

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Comman d Injection')			/goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root.		
			CVE ID : CVE-2023- 23295		
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023-	N/A	O-KOR-JETW- 170323/1266
Droduct, jot	wave_2114_fir	2010/00/00	23296		
-	sion(s): * Up to		g) 1.4		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294	N/A	O-KOR-JETW- 170323/1267
Improper Neutralizat ion of Special Elements used in a Command ('Comman	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd	N/A	O-KOR-JETW- 170323/1268

0-1

1-2

2-3 3-4 4-5 Page **807** of **859** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			parameter in order to execute commands as root.		
			CVE ID : CVE-2023- 23295		
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t.	N/A	0-KOR-JETW- 170323/1269
			CVE ID : CVE-2023- 23296		
Product: jet	wave_2211c_fi	rmware	-		
Affected Ver	sion(s): * Up to	(excluding	g) 1.6		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294	N/A	0-KOR-JETW- 170323/1270
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root.	N/A	O-KOR-JETW- 170323/1271

0-1

1-2

2-3

3-4 4-5 Page **808** of **859** 6-7 7-8

5-6

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23295		
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	O-KOR-JETW- 170323/1272
Product: jet	wave_2212g_f	irmware			
Affected Ver	sion(s): 1.3.t				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294	N/A	O-KOR-JETW- 170323/1273
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	O-KOR-JETW- 170323/1274

0-1

1-2

2-3

3-4 4-5 Page **809** of **859** 5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	O-KOR-JETW- 170323/1275
Product: jet	wave_2212s_fi	rmware			
Affected Ver	sion(s): 1.3.0				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294	N/A	0-KOR-JETW- 170323/1276
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	O-KOR-JETW- 170323/1277
Uncontroll ed Resource	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series	N/A	O-KOR-JETW- 170323/1278

0-1

1-2

2-3 3-4 4-5 Page **810** of **859** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumpti on			1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023-		
			23296		
-	wave_2212x_f	irmware			
Affected Ver	sion(s): 1.3.0				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023-	N/A	O-KOR-JETW- 170323/1279
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	23294 Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	O-KOR-JETW- 170323/1280
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via	N/A	O-KOR-JETW- 170323/1281

0-1

1-2

2-3

5-6 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/goform/formDefaul t. CVE ID : CVE-2023-		
			23296		
-	wave_2411l_fi				
Affected Ver	sion(s): * Up to	(excluding		[
Improper Neutralizat ion of Special Elements used in a Command ('Comman d	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root.	N/A	0-KOR-JETW- 170323/1282
Injection')			CVE ID : CVE-2023- 23294		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	O-KOR-JETW- 170323/1283
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t.	N/A	O-KOR-JETW- 170323/1284

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Des	criptior	n & CVE II	D	Patch		NCIIPC ID
			CVE 2329		/E-2023	3-			
Product: jet	wave_2411_fir	mware							
Affected Vers	sion(s): * Up to	(excludin	g) 1.5						
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	4200 JetW 1.6.0 to Co Injec can r file_r to ex comr	ave 30 are vu omman ction. A nodify name p cecute mands ID : CV	s 1.3.0 a 00 Serie Ilnerable Id In attack	es e xer N er	/A		0-KOR-JETW- 170323/1285
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	4200 JetW 1.6.0 to Co Injec /gofo d. An modi parat to ex comr	ave 30 are vu omman ction vi orm/fo attack ify the meter cecute mands ID : CV	s 1.3.0 a 00 Serie Ilnerable Id a ormSysC	es e Cm N	/A		O-KOR-JETW- 170323/1286
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	4200 JetW 1.6.0 to De via /gofo t.	ave 32 are vu enial of orm/fc ID : CV	Wave s 1.3.0 a 00 Serie Ilnerabl f Service ormDefa /E-202 3	es e N ul	/A		O-KOR-JETW- 170323/1287
Product: jetwave_2414_firmware									
CVSS Scoring S	icale 0-1	1-2 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
Affected Vers	sion(s): * Up to	(excludin	g) 1.4		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294	N/A	O-KOR-JETW- 170323/1288
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	O-KOR-JETW- 170323/1289
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	O-KOR-JETW- 170323/1290
-	wave_2424_fir				
Affected Vers	sion(s): * Up to	excluding			
Improper Neutralizat	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and	N/A	O-KOR-JETW- 170323/1291
CVSS Scoring S	icale 0-1	1-2 2	-3 3-4 4-5 5 Page 814 of 859	-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Comman d Injection')			JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	O-KOR-JETW- 170323/1292
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	0-KOR-JETW- 170323/1293
	wave_2460_fir		-		
	sion(s): * Up to	(excluding			
Improper Neutralizat ion of Special Elements	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command	N/A	O-KOR-JETW- 170323/1294

 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 in a Command ('Comman d Injection')			Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	O-KOR-JETW- 170323/1295		
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	O-KOR-JETW- 170323/1296		
-	wave_3220_v3						
	Affected Version(s): * Up to (excluding) 1.7						
Improper Neutralizat ion of Special Elements used in a Command ('Comman	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter	N/A	O-KOR-JETW- 170323/1297		

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			to execute commands as root.		
			CVE ID : CVE-2023- 23294		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	O-KOR-JETW- 170323/1298
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	O-KOR-JETW- 170323/1299
Product: jet	wave_3420_v3	_firmwa	re	<u> </u>	
Affected Ver	sion(s): * Up to	(excluding	g) 1.7		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root.	N/A	O-KOR-JETW- 170323/1300

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23294		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	O-KOR-JETW- 170323/1301
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	O-KOR-JETW- 170323/1302
Product: jet	wave_4221hp	e_firmw	are		
Affected Ver	sion(s): * Up to	(including	g) 1.3.0		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. CVE ID : CVE-2023- 23294	N/A	O-KOR-JETW- 170323/1303

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. CVE ID : CVE-2023- 23295	N/A	0-KOR-JETW- 170323/1304
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t. CVE ID : CVE-2023- 23296	N/A	0-KOR-JETW- 170323/1305
Vendor: Lin	ux				
Product: lin	ux_kernel				
Affected Ver	sion(s): -			-	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Feb-2023	7.5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (//) to view arbitrary files on the system. IBM X-Force ID: 246333	https://www.i bm.com/supp ort/pages/no de/6953521, https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 46333	0-LIN-LINU- 170323/1306

0-1

1-2

2-3

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24960		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Crafter Studio on Linux, MacOS, Windows, x86, ARM, 64 bit allows SQL Injection.This issue affects CrafterCMS v4.0 from 4.0.0 through 4.0.1, and v3.1 from 3.1.0 through 3.1.26. CVE ID : CVE-2023- 26020	https://docs.c raftercms.org /en/4.0/secur ity/advisory.h tml#cv- 2023021701	O-LIN-LINU- 170323/1307
Cleartext Storage of Sensitive Informatio n	17-Feb-2023	5.5	IBM InfoSphere Information Server 11.7 could allow a local user to obtain sensitive information from a log files. IBM X-Force ID: 246463. CVE ID : CVE-2023- 24964	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 46463, https://www.i bm.com/supp ort/pages/no de/6953519	O-LIN-LINU- 170323/1308
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	5.4	IBM Aspera Faspex 4.4.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials	https://www.i bm.com/supp ort/pages/no de/6952319, https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 44117	O-LIN-LINU- 170323/1309

0-1

1-2

2-3

3-4 4-5 Page **820** of **859** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			disclosure within a trusted session. IBM X-Force ID: 244117.					
			CVE ID : CVE-2023- 22868					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247646. CVE ID : CVE-2023- 25928	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 47646, https://www.i bm.com/supp ort/pages/no de/6956598	0-LIN-LINU- 170323/1310			
Affected Ver	sion(s): * Up to	(excluding						
NULL Pointer Dereferenc e	28-Feb-2023	5.5	In the Linux kernel before 5.16.3, drivers/usb/dwc3/d wc3-qcom.c misinterprets the dwc3_qcom_create_u rs_usb_platdev return value (expects it to be NULL in the error case, whereas it is actually an error pointer). CVE ID : CVE-2023- 22999	https://github .com/torvalds /linux/commi t/b52fe2dbb3 e655eb14830 00adfab68a21 9549e13	0-LIN-LINU- 170323/1311			
Affected Ver	Affected Version(s): * Up to (excluding) 5.17							
N/A	28-Feb-2023	7.8	In the Linux kernel before 5.17, an error	https://github .com/torvalds	O-LIN-LINU- 170323/1312			

0-1

1-2

2-33-44-5Page 821 of 859

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			path in dwc3_qcom_acpi_reg ister_core in drivers/usb/dwc3/d wc3-qcom.c lacks certain platform_device_put and kfree calls.	/linux/commi t/fa0ef93868a 6062babe114 4df2807a8b1 d4924d2	
			CVE ID : CVE-2023- 22995		
Affected Vers	sion(s): * Up to	(excluding	g) 5.17.2		
Missing Release of Resource after Effective Lifetime	28-Feb-2023	5.5	In the Linux kernel before 5.17.2, drivers/soc/qcom/q com_aoss.c does not release an of_find_device_by_no de reference after use, e.g., with put_device. CVE ID : CVE-2023- 22996	https://github .com/torvalds /linux/commi t/4b41a9d0fe 3db5f91078a 380f62f0572c 3ecf2dd	O-LIN-LINU- 170323/1313
Affected Vers	sion(s): * Up to	(excluding	g) 6.0	I	
NULL Pointer Dereferenc e	28-Feb-2023	5.5	In nf_tables_updtable, if nf_tables_table_enabl e returns an error, nft_trans_destroy is called to free the transaction object. nft_trans_destroy() calls list_del(), but the transaction was never placed on a list the list head is all zeroes, this results in a NULL pointer dereference. CVE ID : CVE-2023- 1095	https://github .com/torvalds /linux/commi t/580077855 a40741cf5117 66129702d97 ff02f4d9, https://bugzil la.redhat.com /show_bug.cgi ?id=2173973	O-LIN-LINU- 170323/1314
Affected Vers	sion(s): * Up to	(excluding	g) 6.0.3	1	1

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Interpretat ion Conflict	28-Feb-2023	5.5	In the Linux kernel before 6.0.3, drivers/gpu/drm/vi rtio/virtgpu_object.c misinterprets the drm_gem_shmem_ge t_sg_table return value (expects it to be NULL in the error case, whereas it is actually an error pointer). CVE ID : CVE-2023- 22998	https://github .com/torvalds /linux/commi t/c24968734a bfed81c8f93d c5f44a7b7a9a ecadfa	O-LIN-LINU- 170323/1315
Affected Ver	sion(s): * Up to	(excluding	g) 6.1.13		
Double Free	25-Feb-2023	7.8	In the Linux kernel before 6.1.13, there is a double free in net/mpls/af_mpls.c upon an allocation failure (for registering the sysctl table under a new location) during the renaming of a device. CVE ID : CVE-2023- 26545	https://github .com/torvalds /linux/commi t/fda6c89fe3d 9aca073495a 664e1d5aea2 8cd4377	O-LIN-LINU- 170323/1316
Affected Ver	sion(s): * Up to	(excluding	g) 6.1.2	L	
NULL Pointer Dereferenc e	28-Feb-2023	5.5	In the Linux kernel before 6.1.2, kernel/module/deco mpress.c misinterprets the module_get_next_pag e return value (expects it to be NULL in the error case, whereas it is actually an error pointer).	https://github .com/torvalds /linux/commi t/45af1d7aae 7d5520d2858 f8517a13426 46f015db	O-LIN-LINU- 170323/1317

0-1

1-2

2-3 3-4 4-5 Page 823 of 859 5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22997		
Affected Ver	sion(s): * Up to	(excludin	g) 6.2		
Use After Free	28-Feb-2023	7.8	There is a use-after- free vulnerability in the Linux Kernel which can be exploited to achieve local privilege escalation. To reach the vulnerability kernel configuration flag CONFIG_TLS or CONFIG_XFRM_ESPI NTCP has to be configured, but the operation does not require any privilege. There is a use-after-free bug of icsk_ulp_data of a struct inet_connection_sock . When CONFIG_TLS is enabled, user can install a tls context (struct tls_context) on a connected tcp socket. The context is not cleared if this socket is disconnected and reused as a listener. If a new socket is created from the listener, the context is inherited and vulnerable. The setsockopt TCP_ULP operation does not require any privilege. We recommend	https://git.ker nel.org/pub/s cm/linux/ker nel/git/torval ds/linux.git/c ommit/?id=2c 02d41d71f90 a5168391b6a 5f2954112ba 2307c, https://kernel .dance/#2c02 d41d71f90a5 168391b6a5f 2954112ba23 07c	O-LIN-LINU- 170323/1318

0-1

1-2

2-33-44-5Page 824 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrading past commit 2c02d41d71f90a516 8391b6a5f2954112b a2307c		
			CVE ID : CVE-2023- 0461		
Affected Ver	sion(s): * Up to	(excluding	g) 6.2.0	•	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	22-Feb-2023	5.7	An issue was discovered in the Linux kernel through 6.2.0-rc2. drivers/tty/vcc.c has a race condition and resultant use-after- free if a physically proximate attacker removes a VCC device while calling open(), aka a race condition between vcc_open() and vcc_remove(). CVE ID : CVE-2023- 23039	https://lkml.o rg/lkml/2023 /1/1/169	O-LIN-LINU- 170323/1319
Affected Ver	sion(s): * Up to	(including	g) 6.1.12		
Integer Overflow or Wraparoun d	21-Feb-2023	7.8	afu_mmio_region_get _by_offset in drivers/fpga/dfl-afu- region.c in the Linux kernel through 6.1.12 has an integer overflow. CVE ID : CVE-2023- 26242	https://patch work.kernel.o rg/project/lin ux- fpga/patch/2 02302060543 26.89323-1- k1rh4.lee@gm ail.com	O-LIN-LINU- 170323/1320
Affected Ver	sion(s): 6.0.8				
Use After Free	25-Feb-2023	7.8	In the Linux kernel 6.0.8, there is a use- after-free in run_unpack in fs/ntfs3/run.c,	N/A	0-LIN-LINU- 170323/1321

8					(
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
			related to a difference between NTFS sector size and media sector size.		
			CVE ID : CVE-2023- 26544		
Use After Free	26-Feb-2023	7.8	In the Linux kernel 6.0.8, there is a use- after-free in inode_cgwb_move_to _attached in fs/fs- writeback.c, related to list_del_entry_valid. CVE ID : CVE-2023- 26605	N/A	0-LIN-LINU- 170323/1322
Use After Free	26-Feb-2023	7.8	In the Linux kernel 6.0.8, there is a use- after-free in ntfs_trim_fs in fs/ntfs3/bitmap.c. CVE ID : CVE-2023- 26606	N/A	0-LIN-LINU- 170323/1323
Out-of- bounds Read	26-Feb-2023	7.1	In the Linux kernel 6.0.8, there is an out- of-bounds read in ntfs_attr_find in fs/ntfs/attrib.c. CVE ID : CVE-2023- 26607	N/A	O-LIN-LINU- 170323/1324
Affected Ver	sion(s): 6.2		20007		
Use After Free	28-Feb-2023	7.8	There is a use-after- free vulnerability in the Linux Kernel which can be exploited to achieve local privilege escalation. To reach the vulnerability kernel configuration flag CONFIG_TLS or	https://git.ker nel.org/pub/s cm/linux/ker nel/git/torval ds/linux.git/c ommit/?id=2c 02d41d71f90 a5168391b6a 5f2954112ba 2307c,	O-LIN-LINU- 170323/1325

0-1

1-2

2-33-44-5Page 826 of 859

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CONFIG_XFRM_ESPI NTCP has to be configured, but the operation does not require any privilege. There is a use-after-free bug of icsk_ulp_data of a struct inet_connection_sock . When CONFIG_TLS is enabled, user can install a tls context (struct tls_context) on a connected tcp socket. The context is not cleared if this socket is disconnected and reused as a listener. If a new socket is created from the listener, the context is inherited and vulnerable. The setsockopt TCP_ULP operation does not require any privilege. We recommend upgrading past commit 2c02d41d71f90a516 8391b6a5f2954112b a2307c CVE ID : CVE-2023-	https://kernel .dance/#2c02 d41d71f90a5 168391b6a5f 2954112ba23 07c	
			0461		
Missing Release of Memory after Effective Lifetime	23-Feb-2023	5.5	A flaw possibility of memory leak in the Linux kernel cpu_entry_area mapping of X86 CPU data to memory was	https://git.ker nel.org/linus/ 97e3d26b5e5f 371b3ee223d 94dd123e6c4 42ba80	O-LIN-LINU- 170323/1326

0-1

1-2

3-4 4-5 Page **827** of **859** 5-6

6-7

7-8

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			found in the way user can guess location of exception stack(s) or other important data. A local user could use this flaw to get access to some important data with expected location in memory. CVE ID : CVE-2023- 0597		
Affected Ver	sion(s): 6.2.0				
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	22-Feb-2023	5.7	An issue was discovered in the Linux kernel through 6.2.0-rc2. drivers/tty/vcc.c has a race condition and resultant use-after- free if a physically proximate attacker removes a VCC device while calling open(), aka a race condition between vcc_open() and vcc_remove(). CVE ID : CVE-2023- 23039	https://lkml.o rg/lkml/2023 /1/1/169	O-LIN-LINU- 170323/1327
Affected Ver	sion(s): From (i	ncluding)	5.6 Up to (excluding) 5.	.10.161	
Use After Free	17-Feb-2023	5.5	Due to a vulnerability in the io_uring subsystem, it is possible to leak kernel memory information to the user process. timens_install calls current_is_single_thr eaded to determine if	https://git.ker nel.org/pub/s cm/linux/ker nel/git/stable /linux.git/com mit/io_uring? h=linux- 5.10.y&id=78 8d0824269be f539fe31a785	O-LIN-LINU- 170323/1328

0-1

1-2

2-33-44-5Page 828 of 859

5-6

6-7

8-9

	<pre>the current process is single-threaded, but this call does not consider io_uring's io_worker threads, thus it is possible to insert a time namespace's vvar page to process's memory space via a page fault. When this time namespace is destroyed, the vvar page is also freed, but not removed from the process' memory, and a next page allocated by the kernel will be still available from the user-space process and can leak memory contents via this (read-only) use- after-free vulnerability. We recommend upgrading past version 5.10.161 or commit 788d0824269bef539 fe31a785b1517882e afed93 https://git.kernel.or g/pub/scm/linux/ke rnel/git/stable/linux .git/commit/io_uring</pre>	b1517882eafe d93, https://kernel .dance/#788d 0824269bef5 39fe31a785b1 517882eafed9 3	
Vendor: Microsoft			
Product: windows			
Affected Version(s): -			

0-1

1-2

2-3

3-4 4-5 Page **829** of **859** 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorizati on Bypass Through User- Controlled Key	17-Feb-2023	8.8	Improper Input Validation, Authorization Bypass Through User-Controlled Key vulnerability in Kron Tech Single Connect on Windows allows Privilege Abuse. This issue affects Single Connect: 2.16. CVE ID : CVE-2023- 0882	https://docs.k rontech.com/s ingleconnect- 2-16/update- patch-rdp- proxy-idor- vulnerability	O-MIC-WIND- 170323/1329
Use After Free	22-Feb-2023	8.8	Use after free in WebRTC in Google Chrome on Windows prior to 110.0.5481.177 allowed a remote attacker who convinced the user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) CVE ID : CVE-2023- 0932	https://chrom ereleases.goog leblog.com/20 23/02/stable- channel- desktop- update_22.ht ml	O-MIC-WIND- 170323/1330
Improper Control of Generation of Code ('Code Injection')	24-Feb-2023	7.8	A vulnerability has been found in MarkText up to 0.17.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the component WSH JScript Handler. The manipulation leads to code injection. Local access is	N/A	O-MIC-WIND- 170323/1331

0-1

1-2

2-3

3-4 4-5 Page **830** of **859** 6-7

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-221737 was assigned to this vulnerability. CVE ID : CVE-2023- 1004		
Improper Initializatio n	26-Feb-2023	7.8	A vulnerability, which was classified as critical, has been found in TechPowerUp Ryzen DRAM Calculator 1.2.0.5. This issue affects some unknown processing in the library WinRing0x64.sys. The manipulation leads to improper initialization. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB- 221807. CVE ID : CVE-2023- 1048	N/A	O-MIC-WIND- 170323/1332
Out-of- bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in	https://helpx. adobe.com/se curity/produc ts/after_effect s/apsb23- 02.html	O-MIC-WIND- 170323/1333

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22237		
Improper Input Validation	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21574	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	O-MIC-WIND- 170323/1334
Out-of- bounds Write	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	0-MIC-WIND- 170323/1335

0-1

1-2

2-3

3-4 4-5 Page **832** of **859** 5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2023- 21575		
Out-of- bounds Write	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21576	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	0-MIC-WIND- 170323/1336
Out-of- bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22238	https://helpx. adobe.com/se curity/produc ts/after_effect s/apsb23- 02.html	O-MIC-WIND- 170323/1337

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22239	https://helpx. adobe.com/se curity/produc ts/after_effect s/apsb23- 02.html	O-MIC-WIND- 170323/1338
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Stack- based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22243	https://helpx. adobe.com/se curity/produc ts/animate/ap sb23-15.html	O-MIC-WIND- 170323/1339
Use After Free	17-Feb-2023	7.8	Adobe Premiere Rush version 2.6 (and earlier) is affected by a Use	https://helpx. adobe.com/se curity/produc ts/premiere_r	O-MIC-WIND- 170323/1340

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22244	ush/apsb23- 14.html	
Use After Free	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22246	https://helpx. adobe.com/se curity/produc ts/animate/ap sb23-15.html	O-MIC-WIND- 170323/1341
Out-of- bounds Write	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the	https://helpx. adobe.com/se curity/produc ts/framemake r/apsb23- 06.html	O-MIC-WIND- 170323/1342

0-1

1-2

2-33-44-5Page 835 of 859

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2023- 21619		
Improper Privilege Manageme nt	16-Feb-2023	7.8	A vulnerability has been identified that, if exploited, could result in a local user elevating their privilege level to NT AUTHORITY\SYSTE M on a Citrix Virtual Apps and Desktops Windows VDA.	https://suppo rt.citrix.com/a rticle/CTX477 616/citrix- virtual-apps- and-desktops- security- bulletin-for- cve20232448	0-MIC-WIND- 170323/1343
			CVE ID : CVE-2023- 24483	3	
Improper Input Validation	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21621	https://helpx. adobe.com/se curity/produc ts/framemake r/apsb23- 06.html	O-MIC-WIND- 170323/1344
Out-of- bounds Write	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (and	https://helpx. adobe.com/se curity/produc	O-MIC-WIND- 170323/1345

0-1

1-2

2-33-44-5Page 836 of 859

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21622	ts/framemake r/apsb23- 06.html	
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by a Stack- based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	O-MIC-WIND- 170323/1346
Out-of- bounds Write	17-Feb-2023	7.8	22226 Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	O-MIC-WIND- 170323/1347

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22227		
Improper Input Validation	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22228	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	O-MIC-WIND- 170323/1348
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user.	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	O-MIC-WIND- 170323/1349

0-1

1-2

2-33-44-5Page 838 of 859

7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22229		
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22230	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	0-MIC-WIND- 170323/1350
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Premiere Rush version 2.6 (and earlier) is affected by a Stack- based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx. adobe.com/se curity/produc ts/premiere_r ush/apsb23- 14.html	0-MIC-WIND- 170323/1351

0-1

1-2

2-33-44-5Page 839 of 859

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. CVE ID : CVE-2023- 22234		
Out-of- bounds Write	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Heap- based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22236	https://helpx. adobe.com/se curity/produc ts/animate/ap sb23-15.html	O-MIC-WIND- 170323/1352
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Feb-2023	7.5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (//) to view arbitrary files on the system. IBM X-Force ID: 246333 CVE ID : CVE-2023- 24960	https://www.i bm.com/supp ort/pages/no de/6953521, https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 46333	O-MIC-WIND- 170323/1353
Improper Neutralizat	22-Feb-2023	7.2	VMware Carbon Black App Control	https://www. vmware.com/	0-MIC-WIND- 170323/1354

0-1

1-2

3-4 4-5 2-3 Page 840 of 859

6-7

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')			8.7.x prior to 8.7.8, 8.8.x prior to 8.8.6, and 8.9.x.prior to 8.9.4 contain an injection vulnerability. A malicious actor with privileged access to the App Control administration console may be able to use specially crafted input allowing access to the underlying server operating system. CVE ID : CVE-2023- 20858	security/advis ories/VMSA- 2023- 0004.html	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Crafter Studio on Linux, MacOS, Windows, x86, ARM, 64 bit allows SQL Injection.This issue affects CrafterCMS v4.0 from 4.0.0 through 4.0.1, and v3.1 from 3.1.0 through 3.1.26. CVE ID : CVE-2023- 26020	https://docs.c raftercms.org /en/4.0/secur ity/advisory.h tml#cv- 2023021701	O-MIC-WIND- 170323/1355
Out-of- bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of- bounds read	https://helpx. adobe.com/se curity/produc ts/photoshop	0-MIC-WIND- 170323/1356

0-1

1-2

2-33-44-5Page 841 of 859

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21577	/apsb23- 11.html	
Out-of- bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of- bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21578	https://helpx. adobe.com/se curity/produc ts/photoshop /apsb23- 11.html	O-MIC-WIND- 170323/1357
Out-of- bounds Read	17-Feb-2023	5.5	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds read	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	0-MIC-WIND- 170323/1358

0-1

1-2

2-3

3-4 4-5 Page **842** of **859** 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-		
Use After Free	17-Feb-2023	5.5	21583 FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21584	https://helpx. adobe.com/se curity/produc ts/framemake r/apsb23- 06.html	O-MIC-WIND- 170323/1359
NULL Pointer Dereferenc e	17-Feb-2023	5.5	Adobe InDesign versions ID18.1 (and earlier) and ID17.4 (and earlier) are affected by a NULL Pointer Dereference	https://helpx. adobe.com/se curity/produc ts/indesign/a	0-MIC-WIND- 170323/1360

0-1

1-2

2-3

3-4 4-5 Page **843** of **859** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of- service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-	psb23- 12.html	
Out-of- bounds Read	17-Feb-2023	5.5	21593 FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21620	https://helpx. adobe.com/se curity/produc ts/framemake r/apsb23- 06.html	O-MIC-WIND- 170323/1361
Out-of- bounds Read	17-Feb-2023	5.5	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds read vulnerability	https://helpx. adobe.com/se curity/produc ts/after_effect	O-MIC-WIND- 170323/1362

0-1

1-2

2-3

3-4 4-5 Page **844** of **859** 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22233	s/apsb23- 02.html	
Out-of- bounds Read	17-Feb-2023	5.5	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of- bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 22231	https://helpx. adobe.com/se curity/produc ts/bridge/aps b23-09.html	O-MIC-WIND- 170323/1363
Cleartext Storage of Sensitive Informatio n	17-Feb-2023	5.5	IBM InfoSphere Information Server 11.7 could allow a local user to obtain sensitive information	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 46463, https://www.i	O-MIC-WIND- 170323/1364

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from a log files. IBM X-Force ID: 246463. CVE ID : CVE-2023-	bm.com/supp ort/pages/no de/6953519	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	5.4	24964 IBM Aspera Faspex 4.4.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244117. CVE ID : CVE-2023- 22868	https://www.i bm.com/supp ort/pages/no de/6952319, https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 44117	O-MIC-WIND- 170323/1365
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247646. CVE ID : CVE-2023- 25928	https://excha nge.xforce.ibm cloud.com/vul nerabilities/2 47646, https://www.i bm.com/supp ort/pages/no de/6956598	O-MIC-WIND- 170323/1366
Vendor: Red					
Product: en	terprise_linux				

0-1

1-2

2-3

3-4 4-5 Page **846** of **859** 5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 8.0			I	
NULL Pointer Dereferenc e	28-Feb-2023	5.5	In nf_tables_updtable, if nf_tables_table_enabl e returns an error, nft_trans_destroy is called to free the transaction object. nft_trans_destroy() calls list_del(), but the transaction was never placed on a list the list head is all zeroes, this results in a NULL pointer dereference. CVE ID : CVE-2023- 1095	https://github .com/torvalds /linux/commi t/580077855 a40741cf5117 66129702d97 ff02f4d9, https://bugzil la.redhat.com /show_bug.cgi ?id=2173973	O-RED-ENTE- 170323/1367
Affected Ver	sion(s): 9.0		1075		
NULL Pointer Dereferenc e	28-Feb-2023	5.5	In nf_tables_updtable, if nf_tables_table_enabl e returns an error, nft_trans_destroy is called to free the transaction object. nft_trans_destroy() calls list_del(), but the transaction was never placed on a list the list head is all zeroes, this results in a NULL pointer dereference. CVE ID : CVE-2023- 1095	https://github .com/torvalds /linux/commi t/580077855 a40741cf5117 66129702d97 ff02f4d9, https://bugzil la.redhat.com /show_bug.cgi ?id=2173973	O-RED-ENTE- 170323/1368
Vendor: sicl					
Affected Ver)-gent00000_fi	rmware			
			Missing	https://sick.c	O-SIC-FX0
Missing Authentica	20-Feb-2023	9.8	Missing Authentication for	om/psirt	170323/1369
CVSS Scoring S	Scale 0-1	1-2 2	<mark>-3 3-4 4-5 5</mark> Page 847 of 859	-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
tion for Critical Function			Critical Function in SICK FX0-GENT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000. CVE ID : CVE-2023-				
Affected Vers	sion(s): 3.05		23453				
Missing Authentica tion for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GENT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000. CVE ID : CVE-2023- 23453	https://sick.c om/psirt	O-SIC-FX0 170323/1370		
Product: fx0)-gent00010_fi	rmware					
Affected Vers	sion(s): 3.04						
Missing Authentica tion for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GENT v3 Firmware Version V3.04 and V3.05 allows an	https://sick.c om/psirt	0-SIC-FX0 170323/1371		
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	D	escriptio	n & CVE I	D		Patch			NCIIP	C ID
			arb coc ma RK the poi	attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000. CVE ID : CVE-2023- 23453								
Affected Ver	sion(s): 3.05									<u> </u>		
Missing Authentica tion for Critical Function	20-Feb-2023	9.8	Aut Cri SIC Fir V3. allo unj atta arb coo ma RK the pon CV	tical Fun K FX0-C mware ⁷ 04 and ows an orivilege acker to bitrary r le execu liciously 512 con e listene rt 9000.	ed remo achieve	te e to	-	ps://sic /psirt	ek.c		5IC-FX 0323/	
Product: fx()-gpnt00000_f	firmware	;							<u> </u>		
Affected Ver	sion(s): 3.04											
Missing Authentica tion for Critical Function 9.8			Aut Cri SIC Fir V3. allo unj atta arb coo	Missing Authentication for Critical Function in SICK FX0-GPNT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted			-	ps://sic /psirt	k.c		SIC-FX 0323/	
CVSS Scoring S	Scale 0-1	1-2	2-3	3-4	4-5	5-	-6	6-7	7-8	2	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RK512 commands to the listener on TCP port 9000.		
			CVE ID : CVE-2023- 23452		
Affected Ver	sion(s): 3.05				
Missing Authentica tion for Critical Function 9.8		Missing Authentication for Critical Function in SICK FX0-GPNT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000. CVE ID : CVE-2023-	https://sick.c om/psirt	O-SIC-FX0 170323/1374	
Product: fx(<mark>)-gpnt00010_</mark> f	rmware	23452		
Affected Ver					
miceted ver	31011(3). 5.04		Missing	[
Missing Authentica tion for Critical Function	20-Feb-2023	9.8	Authentication for Critical Function in SICK FX0-GPNT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000.	https://sick.c om/psirt	O-SIC-FX0 170323/1375

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID : CVE-2023- 23452			
Affected Ver	sion(s): 3.05					
Missing Authentica tion for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GPNT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000. CVE ID : CVE-2023- 23452	https://sick.c om/psirt	O-SIC-FX0 170323/1376	
Vendor: Te	nda				1	
Product: ac	500_firmware					
Affected Ver	sion(s): 2.0.1.9	\\(1307\\)			
Out-of- bounds Write	ounds 27-Feb-2023 9.8		Tenda AC500 V2.0.1.9(1307) is vulnerable to Buffer Overflow in function fromRouteStatic via parameters entrys and mitInterface.	N/A	O-TEN-AC50- 170323/1377	
			CVE ID : CVE-2023- 25233			
Out-of- bounds Write	27-Feb-2023	9.8	Tenda AC500 V2.0.1.9(1307) is vulnerable to Buffer Overflow in function fromAddressNat via parameters entrys and mitInterface.	N/A	O-TEN-AC50- 170323/1378	

0-1

1-2

2-3

3-4 4-5 Page **851** of **859** 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25234		
Out-of- bounds Write	27-Feb-2023	7.5	Tenda AC500V2.0.1.9(1307) isvulnerable to BufferOverflow in functionformOneSsidCfgSetvia parameter ssid.CVE ID : CVE-2023-25235		O-TEN-AC50- 170323/1379
Product: ax	3_firmware				
Affected Ver	sion(s): 16.03.1	2.11			
Out-of- bounds Write	23-Feb-2023	9.8	Tenda AX3 V16.03.12.11 was discovered to contain a stack overflow via the timeType function at /goform/SetSysTime Cfg. CVE ID : CVE-2023- 24212	N/A	O-TEN-AX3 170323/1380
Product: cp	3_firmware				
Affected Ver	sion(s): * Up to	(including	g) 20220906024_2025		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.221 1041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V2022090602 4_2025 and Tenda IT7-PCS Tenda IT7- PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7- LCS<=V2209020914 and Tenda IT7-PRS	N/A	O-TEN-CP3 170323/1381

0-1

1-2

2-33-44-5Page 852 of 859

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			Tenda IT7- PRS<=V2209020908.						
			CVE ID : CVE-2023- 23080						
Product: cp7_firmware									
Affected Ver	Affected Version(s): * Up to (including) 1.10.00.2211041403								
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	eutralizat n of becial ements sed in a pommand Comman		Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7 Tenda CP7<=V11.10.00.221 1041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V2022090602 4_2025 and Tenda IT7-PCS Tenda IT7- PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7- LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7- PRS<=V2209020908.	N/A	O-TEN-CP7 170323/1382				
			CVE ID : CVE-2023- 23080						
	'-lcs_firmware								
Affected Ver	sion(s): * Up to	(including							
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.221 1041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V2022090602 4_2025 and Tenda IT7-PCS Tenda IT7-	N/A	O-TEN-IT7 170323/1383				

0-1

1-2

5-6

6-7

9-10

²⁻³³⁻⁴⁴⁻⁵Page 853 of 859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7- LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7- PRS<=V2209020908.		
			CVE ID : CVE-2023- 23080		
Product: it7	-pcs_firmware	;			
Affected Ver	sion(s): * Up to	(including	g) 2209020914		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7 Tenda CP7<=V11.10.00.221 1041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V2022090602 4_2025 and Tenda IT7-PCS Tenda IT7- PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7- LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7- PRS<=V2209020908. CVE ID : CVE-2023- 23080	N/A	O-TEN-IT7 170323/1384
	'-prs_firmware				
Affected Ver	sion(s): * Up to	(including			
Improper Neutralizat ion of Special Elements used in a Command	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.221	N/A	O-TEN-IT7 170323/1385

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

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Comman d Injection')			1041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V2022090602 4_2025 and Tenda IT7-PCS Tenda IT7- PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7- LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7- PRS<=V2209020908. CVE ID : CVE-2023- 23080		
Product: w3	0e_firmware		25000		
		25\\(633\	\mathbb{N}		
Out-of- bounds Write	27-Feb-2023	9.8	Tenda Router W30E V1.0.1.25(633) is vulnerable to Buffer Overflow in function fromRouteStatic via parameters entrys and mitInterface. CVE ID : CVE-2023- 25231	N/A	O-TEN-W30E- 170323/1386
Vendor: tot	olink				<u> </u>
Product: a7	100ru_firmwa	re			
Affected Ver	sion(s): 7.4cu.2	313_b201	91024		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	21-Feb-2023	9.8	TOTOLink A7100RU V7.4cu.2313_B20191 024 was discovered to contain a command injection vulnerability. CVE ID : CVE-2023- 24184	N/A	0-T0T-A710- 170323/1387
Improper Neutralizat ion of	16-Feb-2023	9.8	TOTOlink A7100RU(V7.4cu.23 13_B20191024) was	N/A	0-TOT-A710- 170323/1388
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5	-6 6-7 7-8	3 8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Special Elements used in a Command ('Comman d Injection')			discovered to contain a command injection vulnerability via the province parameter at setting/delStaticDhc pRules. CVE ID : CVE-2023- 24236			
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	16-Feb-2023	9.8	TOTOlink A7100RU(V7.4cu.23 13_B20191024) was discovered to contain a command injection vulnerability via the city parameter at setting/delStaticDhc pRules. CVE ID : CVE-2023- 24238	N/A	0-TOT-A710- 170323/1389	
Product: a7	20r_firmware					
Affected Ver	sion(s): 4.1.5cu	.532_b202	210610			
Incorrect Authorizati on	17-Feb-2023	9.8	TOTOLINK A720R V4.1.5cu.532_ B20210610 is vulnerable to Incorrect Access Control. CVE ID : CVE-2023 -	N/A	0-TOT-A720- 170323/1390	
Vendor: Tp-	link		23064			
Product: ar						
	sion(s): v2_160	801				
Improper Resource Shutdown or Release	21-Feb-2023	6.5	A vulnerability was found in TP-Link Archer C50 V2_160801. It has been rated as	N/A	O-TPARCH- 170323/1391	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 856 of 859										

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			problematic. Affected by this issue is some unknown functionality of the component Web Management Interface. The manipulation leads to denial of service. The attack can only be initiated within the local network. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221552. CVE ID : CVE-2023- 0936				
Product: tl-	wr940n_firmw	are					
Use of a Broken or Risky Cryptograp hic Algorithm	22-Feb-2023	7.5	TP-Link router TL- WR940N V6 3.19.1 Build 180119 uses a deprecated MD5 algorithm to hash the admin password used for basic authentication.	https://midist 0xf.medium.co m/tl-wr940n- uses-weak- md5-hashing- algorithm- ae7b589860d	O-TPTL-W- 170323/1392		
			CVE ID : CVE-2023- 23040	2			
Vendor: ui							
Product: unifi_dream_machine_pro_firmware							
Affected Version(s): 7.2.95							
N/A	23-Feb-2023	9.8	Ubiquiti Networks UniFi Dream Machine Pro v7.2.95 allows attackers to bypass domain	N/A	0-UI-UNIF- 170323/1393		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 857 of 859										

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restrictions via crafted packets. CVE ID : CVE-2023- 24104		
Vendor: Zyz	kel				
Product: lte	3202-m437_fi	rmware			
Affected Ver	sion(s): 1.00\\(abwf.1\\])c0		
N/A	21-Feb-2023	9.8	A security misconfiguration vulnerability exists in the Zyxel LTE3316-M604 firmware version V2.00(ABMP.6)C0 due to a factory default misconfiguration intended for testing purposes. A remote attacker could leverage this vulnerability to access an affected device using Telnet. CVE ID : CVE-2023- 22920	https://www. zyxel.com/glo bal/en/suppo rt/security- advisories/zy xel-security- advisory-for- security- misconfigurati on- vulnerability- of-4g-lte- indoor- routers	O-ZYX-LTE3- 170323/1394
Product: Ite		rmware	22920		
	sion(s): 2.00\\()c0		
N/A	21-Feb-2023	9.8	A security misconfiguration vulnerability exists in the Zyxel LTE3316-M604 firmware version V2.00(ABMP.6)C0 due to a factory default misconfiguration intended for testing purposes. A remote attacker could	https://www. zyxel.com/glo bal/en/suppo rt/security- advisories/zy xel-security- advisory-for- security- misconfigurati on- vulnerability- of-4g-lte-	O-ZYX-LTE3- 170323/1395

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to access an affected device using Telnet.	indoor- routers	
			CVE ID : CVE-2023- 22920		

CVSS	Scoring Scale	0-1	1-2

4-5

5-6

6-7

2-3